Radware DDoS Protection Solutions for Financial Services

Financial Services Concerns and Challenges

In the fast-paced world of financial services, the availability of applications and services is a mission-critical requirement. Customer self-service through online applications has become the norm, enabling customers to conveniently perform a wide range of activities. From account management and fund transfers to loan applications and investment transactions, individuals and businesses rely on the seamless functionality of these online platforms. As a result, financial institutions face the ongoing challenge of providing superior-quality service to attract and retain customers in a highly competitive environment.

With financial services heavily dependent on the uninterrupted availability of their online applications, any disruption can have detrimental effects on customer satisfaction, trust, and ultimately, the bottom line. This is where a robust DDoS protection solution plays a crucial role. By proactively defending against and mitigating DDoS attacks, financial institutions can ensure the consistent availability and reliability of their online services, offering customers a seamless experience.

However, the world is now experiencing an unprecedented rise in DDoS attack activity. A convergence of multiple factors has brought together an explosion in DDoS attack size, frequency, and sophistication. The result is a more dangerous and complex threat landscape than ever before.

With financial services heavily dependent on the uninterrupted availability of their online applications, any disruption can have detrimental effects on customer satisfaction, trust, and ultimately, the bottom line."

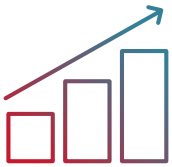
DDoS Attack Campaigns Against Financial Services

While DDoS attacks have been a problem for many years, the past 18 months have seen an unprecedented rise in DDoS attack size and complexity. This new wave of attacks is driven primarily by state-sponsored and hacktivist groups, targeting commercial, governmental and infrastructure targets across many countries.

According to Radware's Attack Hub, which tracks attack activity across its global network, 2022 has seen a year-over-year (YoY) increase of 152% in blocked DDoS events compared to 2021. Similarly, the total blocked volume of DDoS attacks rose by 32% YoY between 2021 and 2022, and the largest DDoS attack observed by Radware in 2022 was 1.46 terabytes per sec (Tbps) in size, a 2.8x increase compared to the largest attack observed in 2021.

Financial institutions such as banks, insurance companies, and financial services organizations have been a prime target as part of these campaigns due to their high visibility, importance, and impact on end users. Indeed, in 2022, the Financial Services Information Sharing and Analysis Center (FS-ISAC) observed a 73% increase in DDoS attacks against financial services organizations in Europe, and a 22% increase in attacks globally.[1]

Between 2021-2022 we observed:



152% Increase in DDoS attacks

73% Increase in DDoS attacks against financial institutions in Europe

22% Increase in DDoS attacks against financial institutions globally

How DDoS Attacks Harm Financial Institutions

DDoS attacks pose a significant threat to the service availability of financial institutions, which is an essential and mission-critical requirement for banks and other financial organizations. These attacks can disrupt the normal functioning of online banking systems, payment gateways, and other self-service platforms that enable customers to access financial services conveniently. This not only hampers customers' ability to perform financial transactions but also erodes their trust in the institution's reliability and security measures. As financial institutions heavily rely on uninterrupted availability to provide seamless services and retain customers, mitigating the impact of DDoS attacks becomes paramount.

[1] FS-ISAC, Navigating Cyber 2023, March 2023. https://www.fsisac.com/hubfs/NavigatingCyber-2023/NavigatingCyber2023-Final.pdf?hsLang=en

DDoS attacks can have significant negative impacts on financial institutions. Here are some ways they can harm these institutions:

Service Disruption

Customers not able to access online banking services, make transactions, or access important financial information.

Financial Loss

Suffer direct revenue loss from lost transactions, fees, new customer signups, etc.

Customer Trust

Loss of customer confidence can have long-term consequences and impact on the organization's business.

Damage to Reputation

Financial institutions rely on their reputation, and DDoS attacks can result in negative publicity and damage to brand.

Customer Churn

Service availability due to DDoS attacks hurts service to customers and may drive them to seek alternatives.

Regulatory Violations

Financial institutions are subject to many regulations. Service unavailability due to DDoS attacks may result in non-compliance.

DDoS attacks can harm financial institutions by causing service disruptions, financial losses, customer trust issues, increased operational costs, and reputational damage. It is crucial for institutions to have robust cybersecurity measures in place to detect, mitigate and respond to such attacks effectively."

The Radware's Solution for Financial Services Industry

Radware's DDoS protection solution for financial institutions offers a comprehensive and tailored approach to safeguarding their critical infrastructure.

Here are the key benefits of Radware's DDoS Protection solution:

- **Protection Against Any DDoS Attack:** Radware's solution provides real-time detection and mitigation of both known and zero-day DDoS attacks, ensuring that financial institutions' networks and services remain accessible and resilient. By leveraging cutting-edge technologies such as behavioral analysis and machine learning, Radware's solution can accurately identify and mitigate all DDoS threats.
- **Scalable and Resilient Infrastructure:** Radware offers a highly scalable, resilient and multi-terabit infrastructure that can handle high-volume DDoS attacks without service disruption. With globally distributed scrubbing centers and intelligent traffic diversion mechanisms, Radware ensures that legitimate traffic reaches financial institutions while malicious traffic is efficiently filtered out.
- **Flexible Deployment Options:** Radware provides financial services institutions with multiple deployment options, including on-premises protection, cloud services, and a hybrid solution that combines on-premises and cloud-based DDoS protection, leveraging the low latency of hardware deployment and the scalability of the cloud.
- **Low False Positives:** Unlike competing solutions, which detect DDoS attacks using volumetric detection or signatures of known attack patterns, Radware uses behavioral-based detection using advanced, patented machine-learning algorithms to protect against known and unknown threats. Radware uses machine-learning algorithms to automatically distinguish between legitimate user traffic and attack traffic. This allows for more accurate detection, with lower rates of false positives.
- **Advanced L7 DDoS protection:** Radware's dedicated Web DDoS protections use advanced L7 behavioral-based detection and mitigation to block sophisticated Web DDoS Tsunami attacks that threaten the availability of web and mobile applications.
- **Integrated Network and Application Protection:** Radware's DDoS protections are integrated within a single cloud solution, so customers can cover all their infrastructure and application protection needs in one integrated solution.
- **Real-Time Threat Intelligence:** Radware's DDoS protections are augmented by multiple threat intelligence feeds that aggregate data from their cloud scrubbing network. Also, a network of dedicated honeypots actively detects new attackers before they ever hit our customers. This way, Radware customers benefit from the crowdsourced intelligence of the entire customer base.
- **Comprehensive Reporting and Analytics:** Radware's solution provides detailed reporting and analytics capabilities, offering financial institutions valuable insights into attack trends, attack mitigation effectiveness, and network performance. These insights enable informed decision-making, continuous improvement of security strategies, and compliance with regulatory requirements.

Managed Services and Attack-Time Protection

Radware's DDoS protection solution is provided as a fully managed service and is supported by Radware's Emergency Response Team (ERT). Radware's ERT provides customers with a single point-of-contact for both their routine and emergency needs, ensuring better security and lower overhead than doing it by themselves.

Radware's Global Scrubbing Network

Radware's Cloud DDoS Protection Service is backed by a worldwide network of 19 scrubbing centers, featuring 12 Tbps of mitigation capacity (and growing). Radware's scrubbing centers are globally connected in full mesh mode, using Anycast-based routing. This ensures that DDoS attacks are mitigated closest to their point of origin, providing truly global DDoS mitigation capable of absorbing even the largest volumetric attacks.

Figure 1

Radware's Global Cloud DDoS Scrubbing Network

Summary

The financial services sector has faced numerous challenges in recent times, particularly with the increased demand for online services and the rise of cyberthreats. However, financial institutions remain vulnerable to DDoS attacks, which can have severe consequences. Such attacks disrupt services, leading to financial losses, customer trust issues, reputational damage, and potential regulatory violations. To address these risks, a comprehensive DDoS protection solution is crucial.

Radware's DDoS protection solution for financial institutions offers precisely that, combining advanced mitigation techniques, scalable infrastructure, hybrid protection, behavioral-based detection, zero-day attack protection, and comprehensive reporting and analytics. With Radware's solution, financial institutions can effectively safeguard their critical infrastructure, ensure uninterrupted service availability, and protect customer trust.

© 2023 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.

RWI 104 18/8/23