Securing the Financial Sector from DDoS Attack

Reducing Risk in an Increasingly Connected World

DDoS Attacks

- The financial sector is a major focus for DDoS attacks.
- A successful DDoS attack can negatively impact revenue, productivity and brand.
- Severity, frequency and complexity of attacks continue to rise.
- DDoS attacks are used as a smokescreen for other APT infiltration/exfiltration activities.
- Criminal gangs, hacktivists and state-sponsored terrorists are involved in initiating DDoS attacks.

Executive Summary

Distributed Denial of Service (DDoS) attacks exhaust network or application resources, impacting the availability of business critical systems and interfaces. DDoS attacks are ever-increasing in sophistication and frequency. Financial institutions have become a key target for criminal gangs and hacktivists, creating a business and regulatory requirement to mitigate this risk. Senior Executives in financial services should take action to reduce business risk. Arbor Networks is an industry leader in helping organisations protect themselves from DDoS attacks, and other network borne threats, and offers a multi-layered approach to securing business infrastructure and services.

A Very Real Threat

DDoS attacks, where a business's servers or network connectivity are flooded with traffic to disrupt normal operations, have become increasingly common in the financial sector. The severity, frequency and complexity of these attacks continue to rise as criminal gangs and state-sponsored terrorists utilise DDoS attacks to further their aims. DDoS attacks can be ideologically, geopolitically or financially motivated and are also now commonly used as a smokescreen for the infiltration/exfiltration activities associated with Advanced Threat (AT) attack campaigns.

Safeguard Customer Trust

From broker-dealers and mutual funds, to insurers and hedge funds, it is important to recognise that customers place enormous trust in financial institutions to protect their investments and personal information. Although DDoS attacks do not usually involve loss of key business data the perception of end-customers and the media can be different, leading to significant brand damage if an attack is successful in disrupting services.

Don't Take Chances—Take Action

The message to Senior Executives is clear—ensuring the availability of IT services is now a board-level concern as the business risks of downtime are significant. Organisations in the financial sector should ensure they have quantified the potential impact of an attack, and that appropriate risk mitigation strategies are in place.

Financial organisations have additional concerns:

- They must demonstrate that their infrastructure complies with regulations.
- Information security regulations are more stringent and far-reaching than in any other sector.
- Critical services, such as core banking and trading applications, must be available at all times.
- Financial institutions offer numerous web services over the internet, creating a direct link between public networks and core business systems.

The High Cost of DDoS Attack

It is imperative that financial organisations protect the availability of their Internet facing services and applications:

- The availability of customer portals, trading and clearing interfaces is imperative—outages can be very costly.
- The risk to business from a successful attack is multi-dimensional and includes revenue loss, reduced operational effectiveness, brand damage and the potential for regulatory fines.
- Service recovery time, after a successful attack, can be significant magnifying the impact of the attack itself. The Scale of the Problem

The most high-profile DDoS attack campaign to date targeting the financial sector was Operation Ababil, which targeted the top 100 US banking institutions. Carried out by a group called Cyber Fighters of Izz ad-Din al-Qassam, the campaign started in September 2012 and lasted over a year. It consisted of multiple waves of attacks, each growing in sophistication and scale.

Analysis showed that hackers studied the defences of their targets and modified their attacks with each wave, sometimes shifting their tactics based on real-time feedback, to better evade mitigation efforts.

In its wake, the Ponemon Institute, sponsored by Arbor Networks, surveyed over 800 IT security practitioners within the finance sector, across North America and EMEA. The research found that financial organisations have on average seven serious cyber-attacks per year, but only 48% believe they have solutions in place that can contain the DDoS threat. Arbor's World-Wide Infrastructure Security Report for 2014 also showed that roughly 1:2 end-user organisations experienced an attack in 2014, with 40% seeing attacks that completely saturate their Internet connectivity.

Questions Senior Executives Must Ask Themselves

- Can I quantify the business risk and associated costs of a successful DDoS attack, or attacks, targeting my key Internet facing services?
- Are threats such as DDoS accounted for with our disaster recovery and business continuity plans?
- Do I have sources of intelligence in place that allow me to understand changes in global/regional/vertical specific attack activity?
- Are we adequately prepared to deal with a DDoS attack?

New Threats Require A New Approach to Security

As an industry leader in the provision of solutions providing defense against DDoS and Advanced Threat attacks, Arbor Networks is a key security partner for many businesses within the finance sector. Arbor's approach is to work with customers to both deliver solutions that will ensure service availability and security, and provide on-going advice and intelligence on threat evolution.

Arbor Networks® SA product portfolio has three areas of focus:

1. **Always-on network perimeter protection from DDoS attacks:** Threats such as DDoS and other cyber-attacks need to be detected and blocked before they escalate into costly service outages.
2. **Cost-effective internal network visibility and threat detection:** The greater your visibility across internal network operations, the better your ability to detect suspicious or malicious activities wherever they occur.
3. **Security analytics:** Speed up the investigation and triage of security events and augment existing threat detection processes with a more proactive 'hunting' approach. Attackers are innovating constantly; maximise the effectiveness of your security resources to counter this innovation by giving them interactive visualisations of key security data, so that threats can be found and contained more quickly.

Arbor Networks strives to be a force multiplier, maximising the effectiveness of existing network and security teams. Our goal is to provide solutions that solve problems and reduced risk, by providing workflows that are focused on user and business requirements.

Learn more about Arbor Networks SA at:
arbornetworks.com/products/sa

The Security Division of NETSCOUT

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

SB/FINANCIALSECTOR/EN/1115-LETTER