MAZEBOLT

DATASHEET

DDoS PROTECTION FOR THE BANKING INDUSTRY

Lower Your Ongoing DDoS Vulnerability Gap to Under 2%

Background

DDoS attacks have been launched against banks for a long time as they make a natural target for cybercriminals. This is mainly due to the fact that they store and transfer large amounts of money online. UK Tesco Bank suffered an attack that resulted in 9000 accounts being compromised and £2.5 million stolen from customer accounts. While the cause of the attack is still under debate, some claim that DDoS attacks targeted contact-less payments on the Tesco mobile app while others claim it was an inside job. A single successful DDoS attack today could cost banks up to $1.8 million.

Research by EY indicates that as DDoS attacks continue to evolve in size, frequency, and sophistication, they are also being used as a smokescreen to hide other serious forms of cybercrimes. Steve Holt, Partner at EY says that their investigations display a growing level of sophistication from hackers trying to defraud banks.

However, more alarming is the fact that ‘1 in 10 banking CEOs don’t know if they’ve been hacked’. This study by KPMG states that banking executives are not inclined to share information about cyber incidents with all their senior staff.

> **“DDoS attacks are akin to staging a protest outside your bank branch, but that could be used as a diversion while the Ocean’s 11 team are climbing up the walls!”**
>
> Bence Horvath, Director of EMEIA Cyber Centre of Excellence, EY

Known Published Attacks on Banks 2019-2020

2020	Europe	Large European Bank	Traffic patterns rose to its peak volume within two minutes and lasted just under 10 minutes.
2020	USA	Chase Bank, Bank of America	Millions hit with the internet, phone, and data outages across the United States.
2020	Australian	Several banks (names unknown)	The Silence Hacking Crew claimed the responsibility of this DDoS ransom threat campaign, but no bank has come forward to share information on an attack.
2019	S. Africa	Several banks (names unknown)	Repeated DDoS attacks with ransom notes causing downtime.
2019	UK	HSBC	Launched two days before the annual Jan. 31 tax payment deadline leading to a 3 percent penalty for millions of tax defaulters.
2019	Chile	Banco de Chile	Corrupted the master boot records (MBRs) of 9,000 PCs and servers, leaving them unable to be rebooted.
2019	Netherlands	ABN Amro	Internet Banking, Mobile Banking, the abnamro.nl website and, iDeal were unavailable or extremely slow.
2019	Indonesia	Bank of Indonesia	Bank Indonesia detected 273 viruses and 67,000 spam emails to its email server and website.

In 2016, the hacktivist group called Anonymous struck at some of the world’s leading banks with its OpIcarus Distributed Denial of Service campaign. Its goal was to take down the websites and services associated with the global financial system. Targets include the New York Stock Exchange, Bank of England, Bank of France, Bank of Greece, Bank of Jordan, and the Bank of South Korea, among others. A target list of more than 160 financial organizations was also published on Pastebin by the group.

The DDoS Problem

A well-executed DDoS attack can interrupt a host of banking services including website access, ATM networks, and online banking platforms, in addition to internal systems and functions that help the bank operate and serve customers. Beyond the operational impact is the resulting damage to the institution's brand equity and reputation when customers are prohibited from accessing their financial information and funds.

Reality or Fiction

Banks most often entrust their security in the hands of DDoS mitigation companies. The challenges being that mitigation solutions do not constantly re-configure and fine-tune their DDoS mitigation policies. There is very limited ongoing visibility of DDoS risks and most importantly they do not detect DDoS attacks before they are launched (reactive only). For these reasons we see so many successful damaging DDoS attacks on banks and financial institutions.

Some banks opt for DDoS testing. The key issues with this is that it tests only human and procedural response handling, not actual DDoS vulnerability coverage. Also it simulates only a small variety of real DDoS attack vectors. It's a static test run on dynamic systems (on average runs twice a year) which makes the information gathered relevant only to that point in time. To top it off it's disruptive to IT systems.

For banks to have end to end full DDoS security, they need to continuously close all major DDoS vulnerabilities. To do so another security layer needs to be added to the current mitigation solution.

How? Introducing RADAR™

RADAR™ simulates DDoS attacks continuously and non-disruptively. Taking a DDoS risk-based approach that prioritizes vulnerabilities to reduce time and effort needed to close the highest risk vulnerabilities.
It's another layer that works on top of any mitigation system installed.

Reducing and maintaining the vulnerability level from an average of 48% to under 2% ongoing.

Benefits of RADAR™ for the Banking Industry

- DDoS RADAR™ empowers the IT heads of banks to identify the number of vulnerabilities closed and % of improvement on an ongoing basis.
- RADAR™ works with any existing DDoS mitigation solution, enabling continuous feedback that detects, controls, and secures infrastructure against the most damaging DDoS vulnerabilities.
- The team can identify vulnerabilities immediately when they get generated across live production web-facing IPs. Then ensuring that sneakier and smaller attacks do not go unnoticed. Providing mitigation vendor(s) with targeted information on where the most crucial vulnerabilities have opened, and how to close them efficiently and quickly.
- MazeBolt offers a holistic view of existing DDoS vulnerabilities across multiple locations and prioritized reports and ongoing alerts of DDoS vulnerabilities. Providing specific reports on how each of your affiliates and branches performed against the group and Industry DDoS risk benchmarks.

About MazeBolt

MazeBolt is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and elimination and working with any mitigation system to provide end to end full coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before an attack happens.

For more information,
please visit: www.mazebolt.com
or e-mail: info@mazebolt.com