MAZEBOLT

WHITEPAPER

DDoS Protection for Top 4 Industry Segments

Banking, Government, Retail, and Telecom

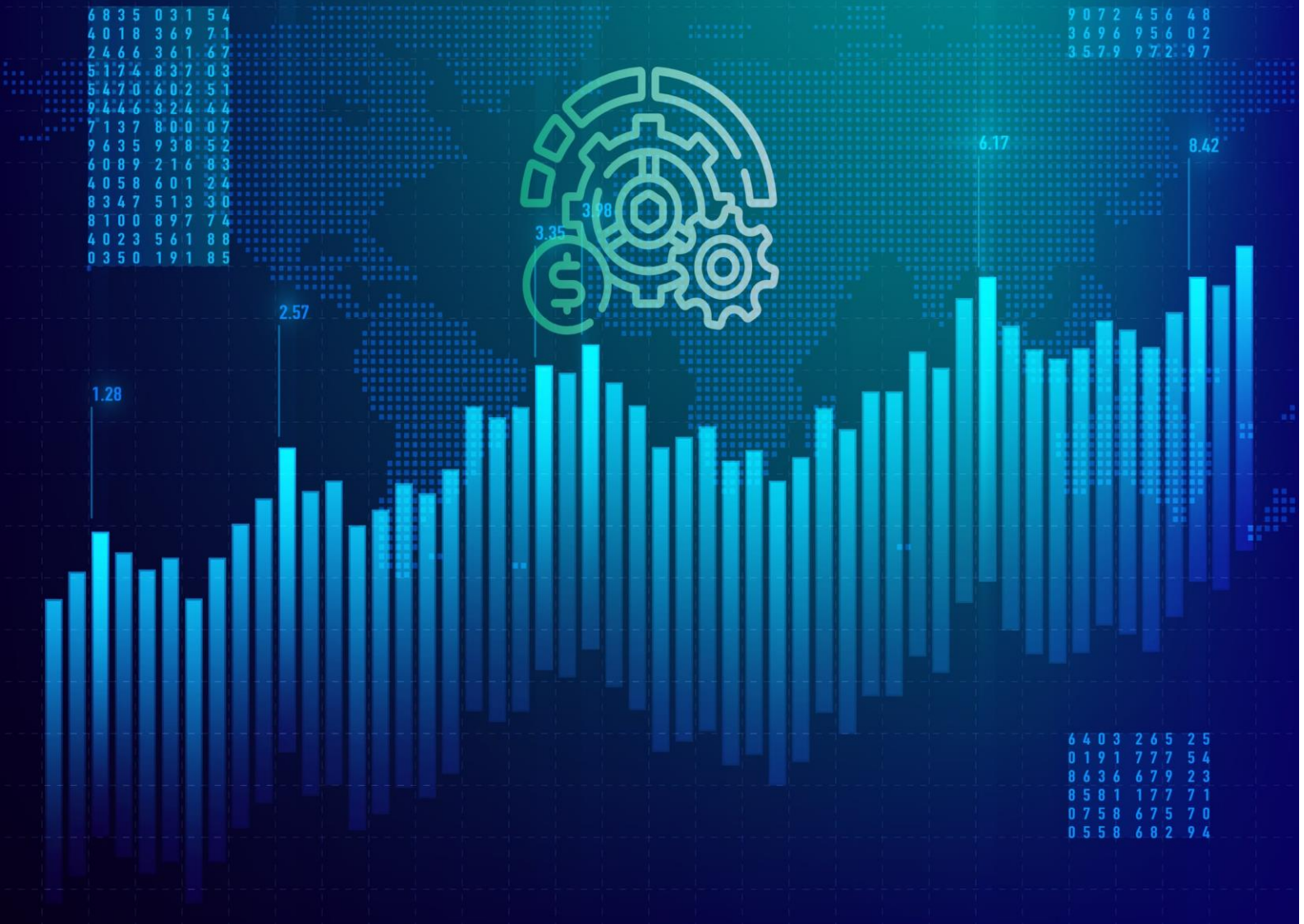

Table of Contents

Banking

Overview

The banking sector has always been a target for application and network layer DDoS attacks and one single attack is all that is required to decrease customer confidence levels. The financial losses are significant and a recent survey by Neustar states that over 80% of companies suffer an estimated loss of $10,000 per hour during a DDoS-related outage. DDoS attacks on banks can cripple online banking services by preventing customers from accessing the site. DDoS attacks can also be used to distract the network team even as other forms of cyber-attacks are executed on internal applications. These kinds of attacks will result in loss of data which is the ethos or the core of banking services. Even one such attack, even without data loss, will result in damage to reputation and customer confidence. For example, during Operation Power Off, several banks reported that during a DDoS attack, the public impact was far greater than financial damage.

Banks most often entrust their security in the hands of DDoS mitigation companies. The challenge is 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) as mentioned in the European case study.

Some banks opt for DDoS testing. The key issues with this are 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 is 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 its disruptive to IT systems.

For banks to have the ultimate DDoS protection, they need to continuously close all major DDoS vulnerabilities. Based on 420 DDoS tests conducted by MazeBolt on enterprises for the first time between 2015 to the end of 2017, configurations leave an inline vulnerability of >48%, empowering DDoS attack vectors to penetrate the best of DDoS mitigation solutions.

CASE STUDY - PAYONEER

Payoneer is a financial services company that offers online money transfer and digital payment services. More than 4 million customers trust Payoneer to receive and manage their international payments.

Challenge: Payoneer's network changes continuously, providing global network access to third parties, adding new mail servers etc. Payoneer did not have the tools to configure DDoS mitigation for the vulnerabilities that may be open due to network changes and result in sneakier DDoS attacks.

Payoneer now uses MazeBolt's RADAR™.
Read case study

"MazeBolt Technologies provides us with real-time views of our DDoS Vulnerabilities, allowing us to mitigate them in a timely manner which was not previously possible."
Yaron Weiss, VP Corporate Security and Global IT Operations (CISO)

DDoS Attacks on Banks

Attackers often launch ransom-related DDoS attacks on banks. In 2020, attackers threatened Australian banks with DDoS attacks if they will not pay large sums in cryptocurrency.

Attackers also often use DDoS attacks to distract the network security team, as they sneak in attacks on applications to steal customer data.

A huge DDoS attack of over 800 million packets every second hit a large European bank. The important point to be noted is how the attack escalated from nearly 400 GB to over 800 GB in less than 120 seconds. The point to be noted is the information shared by the mitigation solution provider after the attack. They said that they were caught by surprise by the unusual aspect of the attack that involved a totally new botnet army.

Government

Overview

Entire countries across the world are going through digital disruption as they digitalize their services to better serve their citizens even as they reduce costs. This largescale transformation comes with its own challenges and governments worldwide find themselves constantly targeted by DDoS attackers. When governmental organizations are impacted by DDoS attacks, the effects are far-reaching, and the damages can be significant. For example, in October 2020, a DDoS attack made the headlines when it prevented the Robert Koch Institute (RKI), Germany's national institute for disease control, from publishing its latest numbers on coronavirus cases. This delay in responding to the pandemic COVID-19 impaired the government's effort to contain the spread of the virus. These attacks continue to happen and continue to catch targets by surprise by their suddenness and intensity.

Mitigation measures often fail in the face of DDoS attacks as seen in the above examples. This is because DDoS attacks are increasingly more complex and quicker. They leave much less time for current DDoS mitigation systems to react. Many DDoS attacks manage to penetrate the best mitigation solutions. To address these challenges, there is a need to detect and close all DDoS vulnerabilities ongoing before an attack is launched. Allowing mitigation solutions to respond in the fastest possible way with minimal manual intervention.

CASE STUDY - GOVERNMENT

This government site hosts services and information from the Prime Minister's Office, the Ministry of Tourism, Culture and Sport, Public Security, Transport and Road Safety, Energy, Construction and Housing and the Law Enforcement and Collection System Authority and so forth.

Challenge: The customer wanted to ensure that its existing infrastructure would not be compromised during the 2019 parliamentary elections due to DDoS attacks. It was critical that the infrastructure displayed seamless performance, reliability, and security always but even more so during peak traffic periods.

Solution: To ensure business continuity, peak performance, and 24/7 availability, MazeBolt evaluated the existing DDoS mitigation postures and suggested the implementation of the DDoS RADAR™, a patented technology that enables Continuous Feedback on top of any DDoS Mitigation system. DDoS vulnerabilities were eliminated and drastically reduced within 2 weeks.

Benefits: DDoS vulnerabilities were eliminated and drastically reduced DDoS risk within 2 weeks. The infrastructure performed at its maximum capacity and ensured that there was no downtime

DDoS Attacks on Governments

Governments worldwide are either impacted or learning from those already affected by DDoS attacks. Recently, the National Action Party or PAN – Mexico's Political Opposition Party – was targeted by DDoS attacks that took down its website for about 15 minutes. Every month, 20 to 40 million attacks are launched against Taiwan's government websites. Millions of Australians were unable to fill out mandatory Census online data forms because the government website was slammed by a Distributed Denial of service (DDoS) attack. Government servers were forced offline in Luxembourg when they came under a DDoS attack.

Politically motivated attacks are aimed to cause the victim damage or register their displeasure with some actions. Attacks often coincide with large-scale public happenings such as elections. Before and during the US elections, political campaigns experienced an average of 4,949 cyber-threats per day, and larger campaigns even more. Government election-related sites were seeing over 122,000 threats every day.

Attackers sometimes are motivated to fight for social and ideological beliefs. In January 2019, Zimbabwean government-related websites were hit with a DDoS attack by the hacktivist group Anonymous protesting internet censorship in the country.

There are also incidents of "state-sponsored" attacks. The 2020 Australian government attacks, targeted Australian businesses and governments. The attacks were described as "state-sponsored", which means a foreign government was believed to be behind it.

Historical data indicates that for DDoS attackers, any large-scale event is an invitation to launch a DDoS attack. In March 2020, the US Department of Health and Human Services was hit by a DDoS attack during the COVID-19 coronavirus pandemic.

Along with political motives, attackers indulge in attacks for cyber extortion demanding ransom in the form of Bitcoin. The attackers demand ransom threatening data exposure or long periods of downtime.

Retail

Overview

As the retail industry continues to transform and adapt to disruptive digital transformations, the threat of DDoS grows. There have also been several instances of ransom threats with DDoS attacks on retailers. Finding customers who buy online, keeping in mind the severe competition, and then losing them to a DDoS attack is unimaginable.

Summarizing this rise in attacks, the Organized Crime report has found DDoS to be a top-five threat emerging from organized crime, for which extortion was the most common motive with DDoS attacks targeting retailers during the peak holiday season.

CASE STUDY - RETAIL

20000 stores across 45 states in the USA, delivering everyday low prices on essential products from America's most trusted brands.

Challenge: Despite having a leading DDoS protection solution, website availability was being impacted by DDoS attacks. These impacts were being discovered at the worst possible time – when the system came under a damaging DDoS attack. The impact was significant, with downtime costing over US$100,000 per hour.

Solution: MazeBolt's RADAR™ solution continuously detected DDoS attacks that bypassed their mitigation solution before the attacks were launched and not after they impacted operations.

Benefits: The continuous visibility provided by RADAR™ highlighted just how critical it is to match network changes (e.g., adding new IP ranges, upgrading network equipment, launching new services, etc.) with respective fine-tuning of DDoS protection policies.

DDoS Attacks on Retail

When Dyn was hit with DDoS, Etsy, Shopify, and PayPal amongst others experienced lengthy outages. The Shopify DDoS attack put several stores out of business.

In 2019, security firms reported a 150 percent increase in DDoS attacks in the months between summer and the end of the year.

Telcos

Overview

With an ever-growing customer-base and technology disruptions, Telcos are encountering constant pressure to deliver innovative services at lower costs to retain their customers in a highly competitive market. Along with facing challenges related to network optimization and performance, technologies such as SDN, 5G, and NFV, they are now encountering the biggest challenge of all times – Distributed Denial of Service attacks (DDoS).

Telcos operate many of the services that are most vulnerable to DDoS attacks such as NTP or DNS, increasing vulnerability levels. Telcos sometimes become the vectors through which large outages are created. If a service provider is attacked and the services allowing them to operate their network are compromised, an entire region can be compromised. Attacks on Telcos can cripple customers' services and temporarily bring them down. For example, during the Dyn DDoS attack, nearly 70 enterprises suffered outages.

CASE STUDY - VAS for TELCOS

Published reports show that DDoS attacks are costing enterprises between $50,000 to $2.5M per attack. In 2020, a large European carrier reported that when an attack is active, up to 70% of their network traffic can be DDoS. In 2020 alone wireless telecommunication companies saw a 64% increase in DDoS attacks.

Telcos are looking for brand differentiators, new revenue streams, and tiered security services. Telcos are also continuously reinventing themselves by enhancing the value they provide and by optimizing customer experience. Telcos can now offer premium DDoS security services to their customers, triggering customer dependability and loyalty.

Why RADAR™

- DDoS attacks are penetrating top mitigation solutions.
- DDoS attack surface risks are constantly changing.
- Provides automated DDoS protection that assesses DDoS vulnerabilities 24/7 on live production systems. Ensuring that installed mitigation systems are up to date on all DDoS vulnerabilities.
- Cutting down the possibilities of harmful and damaging DDoS attacks from 45% to under 2% on an on-going basis.
- Minimizing the risk of downtime to on-line services and websites.

DDoS Attacks on Telcos

September 2020 saw more than a dozen Telcos across Europe being hit by DDoS attacks that targeted their DNS infrastructure. The attacks which went on for over 24 hours were mitigated but their effects have caused wide-scale outages and connectivity challenges.

In 2020, T-Mobile's US network went down, impacting Verizon, AT&T, and other carriers and social media were abuzz with reports of a major DDoS attack. This was never proved, but the fact remains that the consequences of the downtime impacted several service providers, enterprises, and end-users.

These attacks follow in the footsteps of the massive attack on Telstra, which caused the internet to go down for Telstra's customers as the domain name server (DNS) overwhelmed the company's network infrastructure.

In a separate incident in 2020, Iceland country's main telecommunications and co-location hosting services were also hit by a DDoS attack. The media reports that the attack led to a feeling of 'uncertainty', for the first time in history about telecom services in Iceland.

The disruptions caused by the surge in DDoS attacks have left many of the affected countries still reeling under the effect. For example, SwissSign from Switzerland lost a key customer as email provider ProtonMail moved over to the company Let's Encrypt amid the disruption. In France, when SFR and Bouygues Telecom were attacked, media reports claim that internet services were affected with 1000s reporting breakdowns and unusual delays in connecting to websites throughout France.

Introducing RADAR™

Working with any mitigation solution installed, RADAR™ offers superior DDoS coverage and automated DDoS protection. RADAR™ simulates over 100 attack vectors with all public facing IPs 24/7, giving real time visibility to all DDoS vulnerabilities with zero downtime.

Book a Demo Now

About MazeBolt

MazeBolt introduces a new standard in DDoS coverage, automatically detecting, analyzing, and prioritizing remediation across the network, doubling coverage, and virtually eliminating DDoS exposure without shutting down organizational operations. MazeBolt's continuous defense supercharges the performance of CISOs as well as the mitigation service provider.