KEY TAKEAWAYS

DDoS attacks
are growing in frequency, complexity, and size

One DDoS solution represents a
single point of failure
and catastrophic losses when overwhelmed

Neustar SiteProtect
is the ideal primary or complimentary DDoS solution to avoid outages

A Top US Bank Trusts Neustar SiteProtect for Reliable DDoS Protection Depth

What's the best approach to take when you're responsible for minimizing your company's risk and safeguarding their assets during a distributed denial of service (DDoS) attack?

It's the question that haunts every chief information security officer (CISO) across the globe, including one at the head of one of the largest banks in the United States. And for CISOs in the financial services industry, the consequence of a missed step could be disastrous.

Cybercriminals have used a number of reasons to deploy DDoS attacks against the financial services industry, including; interrupting access to online services, access to proprietary information, access to personally identifiable information, and the obvious motive of stealing large amounts of money.

Unfortunately for CISOs, the damages don't end there. They also have to deal with the resource-intensive annoyance of being taken offline, as well as the cascading fallout of brand impairment and loss of customer trust that follows.

To make matters worse, some recent DDoS attacks against financial services companies are state-sponsored and are either plotted with the intention of disrupting the flow of money to competing economies, or used as a means of currency manipulation to affect stock markets and the value of a currency.

As attackers become increasingly determined and emboldened to lash out and launch DDoS strikes with impunity, the question for every CISO in the financial services industry continues to linger:

What do you do when you're responsible for minimizing your company's risk and safeguarding their assets during a DDoS attack?

These statistics from our latest Worldwide DDoS Attacks and Cyber Insights Research Report serve to illustrate what the financial services industry is up against:

86%

of organizations were hit with a DDoS attack

44%

reported malware activation after the attack

33%

suffered customer data loss

28%

encountered ransomware with a DDoS attack – up from 17% in 2016

For years, the answer seemed simple enough – throw a lot of hardware at the problem and lock up a single service vendor. This approach seemed to work until the bad guys caught on and adjusted. Now, the threat has changed, the technology used to launch attacks has changed, and worse, the size of attacks and what organizations can endure has changed. Unfortunately, the threats have overwhelmed defenses that were deemed sufficient not that long ago.

In today's cybersecurity landscape, where DDoS attacks against financial institutions are a certainty and not a possibility, having a single defense solution is no longer sufficient. In fact, a single solution may become a single point of failure for the entire financial services industry. And if any industry knows it's a high-profile target for DDoS attacks, and has a lot to lose – it's the financial services industry.

The first high-profile case of DDoS attacks against the industry occurred in 2012 when a number of well-known banks were ruthlessly targeted and taken offline by a series of high-volumetric attacks that were unprecedented at the time. Despite reports that no data was lost or ATM's taken offline, the attackers gained invaluable insight and knowledge into what it takes to overwhelm their defenses.

Since then, the onslaught against financial institutions has only increased over the years. And for financial institutions that didn't heed the lessons from 2012 and build additional layers of security or redundancy into their systems, history soon would prove itself to be cyclical.

The debut of the Mirai botnet in the fall of 2016 forever changed the paradigm of DDoS attacks. The botnet, which was fueled by insecure Internet of Thing (IoT) devices, began to emerge as a new weapon for DDoS attacks.

With volumetric attacks surpassing 1 Tbps - the largest attack volumes ever seen in the industry - chaos reigned down on organizations across the globe. The most devastating incident occurred on October 21, when Mirai was aimed at a well-known DNS provider. The attack succeeded in not only taking the provider offline, but it also created a ripple effect of downtime for companies that solely relied on the DNS provider for access to critical Internet and infrastructure services.

The effect of the attack was so widespread that many began to wonder if the entire Internet had crashed.

TAKE ACTION

1 **Are you at risk?** Review your current DDoS Protection now to ensure your provider is equipped to defend against massive new volumetric attacks.

2 **Have a better back-up plan.** Ensure you have redundancy built in to your DDoS defense strategy with either dual-DDoS providers or a cloud-failover solution.

To further complicate matters, the sheer size and impact from the Mirai Botnet created a moral and financial dilemma for DDoS mitigation providers. On one hand, they have an obligation to service the attacked company. But in doing so, they would exhaust their mitigation resources, which could affect other clients. And with a number of financial institutions solely depending on one DDoS vendor for protection - much like using only one DNS provider - the possibility of having that vendor become a single point of failure for the entire industry has become a reality.

In effect, the Mirai Botnet solidified the reasoning for employing a complementary or backup DDoS solution.

Seeking to apply lessons learned from previous mistakes, financial institutions are increasingly integrating best practices for building redundancy into their critical networks by either using dual primary DDoS solutions, or employing a secondary or failover DDoS mitigation solution in the event that attacks overwhelm their initial layer of protection.

How Neustar Helps

After the massive DNS outage caused by the Mirai Botnet, Neustar was approached by one of the 3 largest banks in the United States to ensure they had redundancy built into their DDoS defense system.

By turning to Neustar SiteProtect to act as a secondary DDoS solution, our customer was able to implement a robust, on-demand hybrid DDoS defense that's capable of taking over from the customer's primary DDoS mitigation provider in the event of mitigation problems or platform saturation. If the primary DDoS defense system stumbles, Neustar SiteProtect quickly takes over to detect and mitigate attacks while keeping critical systems online without any interruptions.

Our customer designed and provisioned the SiteProtect service to be dynamically customer-triggered, which allowed them to feel secure due to Neustar's local mitigation capabilities. And for this customer, closer mitigation nodes means quicker traffic scrubbing, resulting in less website/application delays and disruptions.

Learn More Today

PHONE

France: 0800-909-776
Germany: 0800-182-8063
UAE: 800-0357-03762
UK: +44-(0)-1784-448-444
US: +1-855-898-0036
Australia: +61-3-9866-3710

EMAIL

APAC: APACSec@team.neustar
EMEA: Euroinfo@team.neustar
North America/other: NASec@team.neustar

It's Time to Diversify Your DDoS Protection

In financial services, the best practice for customers is to diversify their investments to protect against market risks. Now more than ever, this practice should be applied to your DDoS defenses.

You need to reassess your current DDoS mitigation strategy and understand if your provider could become a single point of failure and represent a costly liability to your organization by becoming overwhelmed by a large attack.

Now is the time to diversify your DDoS mitigation solution because we've seen that relying on just one vendor could spell disaster if they are ever overwhelmed or taken down by a massive DDoS attack - or coordinated attacks against multiple financial institutions.

Now is the time to look for either a dual primary or complimentary provider that's equipped with a redundant and robust DDoS mitigation platform that can supplement your initial solution in the event of an emergency.

LEARN MORE

So, what do you do when you're responsible for minimizing your company's risk and safeguarding their assets during a distributed denial of service (DDoS) attack?

You look to Neustar.

Visit us at **www.security.neustar** for more information.

About Neustar.

Every day, the world generates roughly 2.5 quadrillion bits of data. Neustar isolates certain elements and analyzes, simplifies and edits them to make precise and valuable decisions that drive results. As one of the few companies capable of knowing with certainty who is on the other end of every interaction, we're trusted by the world's great brands to make critical decisions some 20 billion times a day. We help marketers send timely and relevant messages to the right people. Because we can authoritatively tell a client exactly who is calling or connecting with them, we make critical real-time responses possible. And the same comprehensive information that enables our clients to direct and manage orders also stops attackers. We know when someone isn't who they claim to be, which helps stop fraud and denial of service before they're a problem. Because we're also an experienced manager of some of the world's most complex databases, we help clients control their online identity, registering and protecting their domain name, and routing traffic to the correct network address. By linking the most essential information with the people who depend on it, we provide more than 11,000 clients worldwide with decisions—not just data.

More information is available at

www.home.neustar

©2017 Neustar, Inc. All rights reserved. All logos, trademarks, servicemarks, registered trademarks, and/or registered servicemarks are owned by Neustar, Inc. All other logos, trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

CS-SEC-85552-08.17.2017