WHITE PAPER

DDoS DISRUPTION IMPACTS

The Need for Always-On Security

neustar®

TABLE OF CONTENTS

INTRODUCTION

While details are murky in terms of what recovery from Covid-19 will look like, one thing is abundantly clear for enterprises around the world: the importance of expanding and securing their digital business footprint. Covid has driven companies to increase remote work and collaboration capabilities, migrate more assets to the cloud, meet customer demand for online interactions and integrate advanced technologies like artificial intelligence (AI), automation, and advanced analytics into operations and business decision making.

Prior to Covid, most companies were somewhere on the path of digital transformation, the ultimate goal of which is to improve business processes and better serve customers. But that path was often elusive, more of a moving target than a well-defined timeline of objectives. As the pandemic forced companies to increase dependence on digital solutions to survive, the result has been an increase in digital transformation timelines by an average of 4-6 years[1].

However, with the acceleration of digital transformation initiatives, there has also been a correlating increase in cyberattacks. This is especially true for distributed denial of service (DDoS) attacks, which are a constant and persistent threat to the availability and security of every organization with a digital presence. Consider, for instance, the following impacts that DDoS has had on enterprise network security in the past year:

- The number of DDoS attacks increased 154% to more than 30,000 attacks per day[2]
- More than 70% of enterprises now report having a DDoS attack[3], up from an average of 52% before the pandemic
- Only 60% of cybersecurity professionals say that the threat data they receive is both timely and actionable[4], and only 29% say the data they receive is both extremely accurate and relevant to the threats their organization is facing at that moment
- With regard to the timeliness of threat data, only 27% of organizations are able to base their security decisions on near real-time data, while 25% say they receive updates hourly and another 24% receive updates several times per day
- DDoS attacks are the greatest concern of security executives

THE CHANGING NATURE OF DDoS

That's not surprising considering that more than 10 million DDoS attacks occurred in 2020[5]. These attacks took place at greater frequency, speed and strength, exhibiting a sophistication and diversity in attack vectors.

DDoS attacks are unique in that their purpose is to make content unavailable, most often in the form of volumetric, protocol-based and application-based assaults. DDoS attacks are generally performed by botnets, a large group of distributed computers that work together to flood a network with malicious traffic and, thus, block legitimate users from access. Botnets can originate from a variety of sources, including compromised computers, mobiles and IoT devices. Because DDoS attacks are distributed in nature, they're much more difficult to control because you can't simply block requests from a single illicit source.

Increasingly, DDoS attacks are being used as a smokescreen to hide even more nefarious activities taking place elsewhere. This is especially harmful to organizations with overtaxed security and IT teams; as they shift all of their attention to combating a DDoS attack, attackers are busy infiltrating the organization in another way. Such was the case in August 2020, when the New Zealand Stock Exchange experienced a DDoS attack[6] over two days, ultimately forcing a shutdown of operations and halting trading. Meanwhile attackers focused their attention on backend infrastructure, application programming interface (API) endpoints, domain name system (DNS) servers and the internet service providers (ISPs) used by the stock exchange.

Another important shift is that DDoS attackers increasingly are reducing the amount of time a DDoS attack lasts—often less than two minutes—while ramping up the frequency of attacks. In many cases, attackers use these high-frequency, low-volume attacks to time how long it takes a company to respond. Subsequent attacks are then built with those response times in mind.

THE PEOPLE FACTOR

Security teams increasingly are being hobbled by their dependence upon fully automated security solutions. In the past, many companies chose security solutions that enabled them to keep all security functions in-house, following the logic that security would be improved by eradicating external personnel involved with security measures.

However, a perfect storm of sorts is forcing companies to rethink that logic. The increase in size, volume and intensity of DDoS attacks is occurring at the same time that there's a massive global shortage of cybersecurity professionals. In early 2019, Gartner estimated there would be a shortage of 2 million cybersecurity professionals[7] by the end of 2019. But the increase in attacks—as well as pressures added for IT and security teams to support workplace shifts brought about by the pandemic—has escalated the skills gap. Moreover, filling those positions is extremely difficult, as the supply of candidates is low, and competition for hiring talent has increased significantly.

As such, 74% of companies are reporting that the skills gap is impacting their ability to secure sensitive information[8], which is leading to data breaches. It's not surprising, then, that companies are choosing to outsource their IT security functions for a number of reasons, including:

- Access to dedicated security specialists who complement internal staff
- Ability to detect and respond quickly to incidents, thus protecting the company's brand and reputation
- Reducing costs by not having to hire cybersecurity professionals, who can demand much higher salaries because they're in such high demand
- Reducing strain on internal IT departments, which increasingly are overwhelmed with the challenges of protecting networks from attack
- Access to the latest technology without having to pay to acquire it and train staff to run it

THE ALWAYS-ON PROPOSITION

Moreover, many companies are moving away from fully automated DDoS mitigation services that are either on-premises or hybrid solutions. These traditional data center models are hobbling companies with high upfront capital costs and limited lifespan of on-premise equipment, as well as the fact that such solutions don't scale well and require repeated investments in hardware.

Likewise, the changes to the nature and severity of DDoS attacks are driving companies to move away from on-demand DDoS mitigation—which requires corporate IT teams to monitor traffic to determine if an attack is happening and then stop it. Instead of struggling alone with fully automated systems to combat DDoS attacks, savvy companies are now embracing always-on, cloud-based DDoS mitigation services like Neustar's UltraDDoS Protect.

UltraDDoS Protect is built on a massive global mitigation platform using best-of-breed technologies. The always-on nature of UltraDDoS Protect enables quick detection and correct reaction to attacks, ensuring that only clean, legitimate traffic is routed to enterprise networks. Moving to an always-on model enables companies to begin protecting in the way that threat actors and bad actors are attacking, responding in a way that fits how attacks are evolving. Instead of fully automated systems that isolate and frustrate security teams, UltraDDoS Protect integrates smart automation and supports customers with a team of cybersecurity professionals who specialize in DDoS mitigation so corporate IT and security teams don't have to.

DDoS attacks have remained a significant threat to enterprise availability for nearly two decades because they are constantly evolving, from simple flood attacks to low volume, difficult to detect multi-vector attacks. This will likely continue as attackers run through a variety of vectors very quickly in order to test where a company does and does not respond well. Moreover, the changing nature of attacks means that many attacks are going unnoticed in the traditional on-demand security scenario. In many instances, an attack may be over before a company can engage its on-demand DDoS provider.

Benefits of Always-On UltraDDoS Protect Include:

Improved Efficiencies

By moving to an always-on threat mitigation solution, companies begin protecting against the way that threat actors are evolving. Attacks have transitioned from single-target, large scale attacks to fast-ramping multi-targeted attacks. Companies need always-on threat mitigation that can detect such attacks, see the bigger picture behind them, and shut them down in their entirety.

Filling the Personnel Gap

The massive shortage of cybersecurity personnel is significantly driving up salaries and lengthening the time it takes to fill open positions. Moreover, corporate IT often spends a disproportionate amount of time watching for attacks in order to trigger DDoS mitigation. UltraDDoS Protect enables companies to leverage a third-party managed service that's staffed by top cybersecurity professionals in the industry. These security experts serve as an extension of your team—enabling your team to focus on IT critical issues like supporting and managing remote workers and automating systems.

True Scalability

Effective network security should easily scale resources according to demand and phase out unnecessary or unused resources when needs fade. UltraDDoS Protect gives companies the ability to respond to attacks in near real time, while protecting against gaps in security. By providing complete visibility and insight into how traffic flows across our infrastructure, we ensure that security resources do not become a bottleneck that impedes network performance and productivity.

Moving From A Capex To Opex Model

There's a false sense of security associated with owning the hardware needed to secure networks. But hardware ownership is a massive capex expenditure, especially given the short lifecycle and constant upgrades needed for network security. UltraDDoS Protect frees IT teams from expensive, capex-intensive hardware and replaces it with an opex-based service with transparent resourcing. Additionally, companies can leverage our relationships with global transit partners worldwide to develop optimum paths of return, further driving down costs while improving security.

INDUSTRIES UNDER ATTACK

While DDoS attacks are leveled against all types of companies, certain vertical markets are highly attractive to attackers: financial services, telecommunications, healthcare, gaming, and e-commerce are at the top of the list. In general, these industries are especially attractive to DDoS attackers because they are so reliant on the availability, performance, and security of digital services. Not only that, many of these industries also have access to sensitive personal information of their customers making them a doubly attractive target.

Telecommunications

Telcos are highly lucrative targets for DDoS attacks because their networks carry traffic for all types of communications, including mobile devices and the Internet of Things (IoT). Telcos build and operate complex networks and store vast amounts of sensitive data about individuals and corporate clients. In many cases, telcos are targeted as they present a gateway into other companies. Additionally, telco networks are vulnerable because they're increasingly adopting public and private cloud services for telco-specific IT applications like customer relationship management (CRM).

Healthcare

The healthcare vertical is vast—insurance providers, hospitals, individual providers, pharmacies, medical equipment providers, research facilities, telemedicine, governmental entities and more. During the pandemic, the healthcare industry has been even more susceptible to DDoS attacks, as resources were focused on combating the virus vs. network security. In fact, nearly a third of hospital staff lacks adequate cybersecurity training[9], and more than 80% of hospital systems have run outdated software during the Covid crisis. Not only do attackers target the healthcare industry to gain access to highly confidential patient data, they also do so to disrupt service availability, disseminate disinformation, and use Ransomware to extort money from providers to make the attacks stop.

Gaming

Because the global pandemic forced people to turn to virtual options for work and play, people turned in droves to gaming as an alternative of hanging out and interacting with friends and family. Not surprisingly, this change caused a massive uptick in the number of DDoS attacks that target the gaming industry, evidenced by a 287% increase in total DDoS attacks against the online gaming and gambling industry[10] during Q3 2020 as compared to the same period in 2019. Gaming businesses face a dual threat. Because the availability and performance of their services are central to their business, they are targets for criminal attackers and extortion schemes. An additional challenge comes from the gamers themselves who are often emotionally engaged, socially active, and often spend disposable income on their gaming accounts. As a result, many have taken full advantage of the democratization of DDoS attacks that took place a decade ago with the rise of Anonymous and the availability of do-it-yourself tools and even DDoS-for hire services. Many gamers are actively using DDoS attacks against their opponents in the hopes of slowing down their services and ability to compete. They take it that seriously.

E-Commerce

E-commerce use exploded during the pandemic, as people were unable to visit brick-and-mortar stores for shopping. Online spending accounted for more than 20% of total retail sales[11] in the US during 2020—growth of more than 15% over 2019 and the highest annual growth in more than two decades. Competition for online dollars is intense, and retailers are investing $5.9B this year in AI-based marketing and customer service solutions to improve shoppers' buying experiences according to IDC. No brand wants to go to those lengths to delight customers and then be embarrassed by an outage caused by a DDoS attack. DDoS attacks not only cause customers to jump ship to competitors, they can increase your marketing costs to win them back. If you become a victim during key sales opportunities like Black Friday and Cyber Monday, the results can be devastating.

Focus On Financial Services

Perhaps no industry vertical is more seemingly lucrative to cyber attackers than financial services, which includes banks, payments companies, card issuers, investment firms, finance companies, money transfer services and more. It's estimated that financial service companies are up to 300 times more likely to experience a cyber-attack[12] when compared to companies in other industries. Furthermore, the cost of a data breach in the financial services sector is $5.85 million[13], as compared to $3.86 million in other industries.

Not surprisingly, the global pandemic has driven up the number of cyberattacks—including DDoS attacks—in the financial services industry, illustrating the vulnerabilities of this vertical and its need for always-on DDoS threat mitigation. In fact, 80% of financial institutions report an increase in cyberattacks[14] since the start of the pandemic.

The situation has become so dire that Jonah Force Hill, Executive Director of the US Secret Service Cyber Investigations Advisory Board, said that in 2020, "Virtually all sectors of the global economy fell victim to cybercrime of one kind or another, but no sector was more regularly targeted than the financial sector. At an alarming rate, transnational organized crime groups leveraged specialist providers of cybercrime tools and services to conduct a wide range of crimes against financial institutions, including ransomware campaigns, DDoS attacks and business email compromise scams."

Companies in the financial services sector are a premier target for DDoS attacks for a number of reasons, including:

- Perception that they have access to large amounts of money
- Attack surface includes core banking IT systems, customer accounts and the wider payment ecosystem
- Access to massive amounts of private data
- High sensitivity to any impact on service
- Complex architectures that are built on a combination of legacy and modern systems, creating potential vulnerabilities
- Required to comply with emerging standards and requirements
- Tends to stay on the cutting edge and drive best practice trends

CONCLUSION

As companies increasingly embrace digitalization, attackers are evolving, as well. Companies that invest in transformative technology will render those investments meaningless if they don't also protect the business, its customers and other vital assets from DDoS attacks. There is too much at stake to continue as if nothing has changed. The time is now to re-evaluate your DDoS defenses.

LEARN MORE

For more information, call **1-855-898-0036 (US)** or **+44 1784 448444 (UK)**, email **securityinfo@team.neustar**, or visit **www.security.neustar**.

APPENDIX

1. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
2. https://securitybrief.co.nz/story/attack-from-dos-in-zero-we-trust
3. https://www.comparitech.com/blog/information-security/ddos-statistics-facts/
4. https://www.securityinfowatch.com/cybersecurity/press-release/21159573/neustar-inc-fewer-than-1-in-3-cybersecurity-professionals-say-threat-data-they-receive-is-extremely-accurate-and-relevant
5. https://www.itproportal.com/news/a-record-number-of-ddos-attacks-took-place-in-2020/
6. https://portswigger.net/daily-swig/new-zealand-stock-exchange-hit-by-series-of-ddos-attacks
7. https://www.gartner.com/en/human-resources/research/talentneuron/labor-market-trends/cybersecurity-labor-shortage-and-covid-19#:~:text=In%20early%202019%2C%20Gartner%20TalentNeuron,has%20further%20escalated%20this%20situation.
8. https://www.prnewswire.com/news-releases/workforce-opportunity-services-hits-the-cybersecurity-skills-gap-head-on-301228486.html#:~:text=A%20study%20by%20eSecurityPlanet.com,and%20issues%20with%20regulatory%20compliance.
9. https://www.forbes.com/sites/forbestechcouncil/2021/12/28/in-good-health-protecting-healthcare-networks-from-cyberattacks/?sh=648fb30d50e0
10. https://www.businesswire.com/news/home/20201215005432/en/Online-Gaming-is-a-Hotbed-for-DDoS-Attacks-According-to-Nexusguard-Research
11. https://www.digitalcommerce360.com/article/us-ecommerce-sales/
12. https://www.bcg.com/en-gb/press/20june2019-global-wealth-report
13. https://www.welivesecurity.com/2021/03/04/cybersecurity-risks-challenges-facing-financial-industry/
14. https://securitybrief.co.nz/story/digital-heists-attacks-on-financial-institutions-rise-238-in-3-months

ABOUT NEUSTAR

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in Marketing, Risk, Communications, and Security that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100. Learn how your company can benefit from the power of trusted connections here: https://www.home.neustar.

WP-SEC-306301-06.09.2021