FS-ISAC Akamai

# DDoS: Here to Stay

March 2024

# Contents

## Executive Summary

In 2023, distributed denial-of-service (DDoS) attacks reached new heights of size and sophistication. The financial sector is the top target across most of the world.

Though DDoS attacks infrequently interrupt internal operations or extract data from mature financial services organizations, they can have an outsized impact on customer confidence. When a website is unavailable – even for seconds – customers can infer that the entire organization is compromised, which damages the firm's reputation.

Much of the upsurge in DDoS attacks beginning in 2022 is attributable to motivated hacktivists, intent on creating as much disruption as they can. Hacktivists use DDoS as a tool of geopolitical conflict and political instability, and will likely continue using that tool as long as it proves effective. Indeed, DDoS attacks increased in 2023 in concert with the outbreak of the Israel-Hamas war and political summits such as the COP 28, during which a noticeable spike in HTTP attacks targeting environmentalist websites was observed.

Along with hacktivists, nation-states, ransomware attackers, and criminal groups all rely on DDoS attacks as part of a layered attack pattern, including as a decoy to divert organizational resources while a threat actor conducts another type of attack. Large-scale DDoS attacks cost little to provision and launch using readily available DDoS-for-hire services and underground markets. It is recommended that financial services organizations optimize their cyber defenses to protect their operations and reputations, and remain compliant as regulations evolve.

## Financial Services: The Top Target for DDoS

Historically, approximately 10%–15% of the DDoS attacks observed by Akamai have been aimed at organizations in the financial services sector. However, since 2021, there has been a distinct and noticeable surge in the number of DDoS attacks against financial services firms.

**DDoS Attacks on Financial Services Firms**

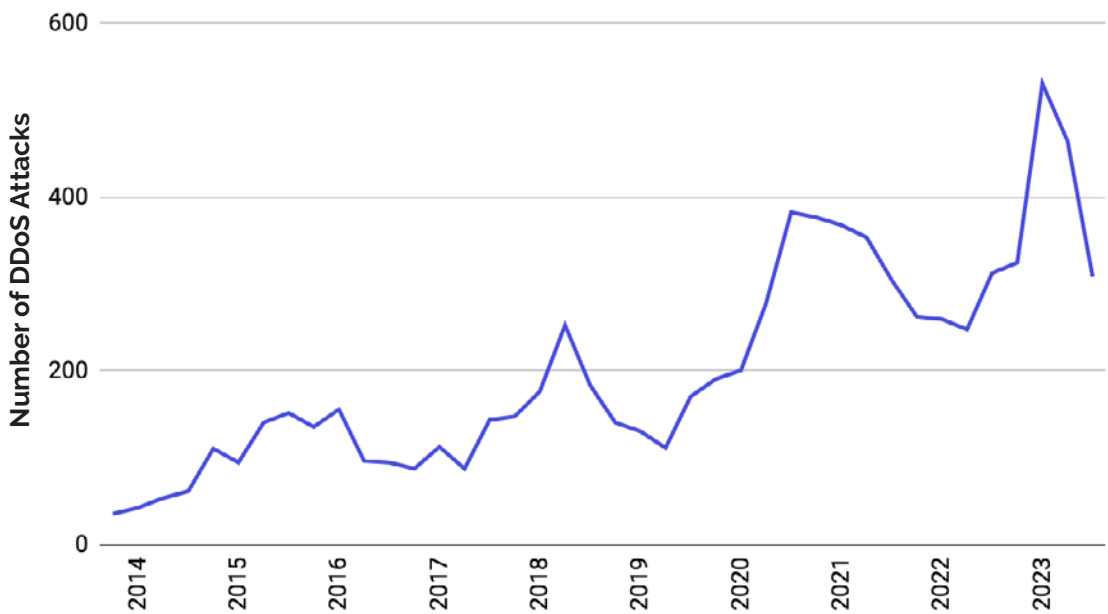



*Figure 1. DDoS attacks on financial services firms. (Source: Akamai)*

According to Akamai data, the number of Layer 3 and Layer 4 DDoS attacks on the financial services sector has increased since 2022, and in 2023 the financial services sector was the prime target of DDoS attacks (Layer 3 and 4). Over a third, 35%, of all attacks on all industries were on financial services institutions in 2023, making the sector a more enticing target than gaming.

Akamai's analysis shows that banking was the target of 63% of DDoS attacks globally. Almost three-quarters (72%) of attacks in EMEA and 91% in APAC were focused on banking. In AMER, however, DDoS attacks were spread more evenly across banking, insurance, and other financial services institutions.

FS-ISAC has seen a corresponding rise between 2023 and 2022; specifically, a 154% year-over-year increase in DDoS reported by members. The rise in reported incidents is in part linked to heightened vigilance following the summer 2023 announcements issued by pro-Russian hacktivist groups of their intentions to launch massive, coordinated DDoS attacks on both European and US financial organizations. FS-ISAC assesses that such announcements led to higher reporting volumes due to the sector's greater vigilance in such periods. However, though the volume of attacks increased significantly in 2023, mitigation measures were successful and no notable impact was reported.

**Financial services saw the most attacks globally (1,986), representing 35.4% of attacks across all verticals**

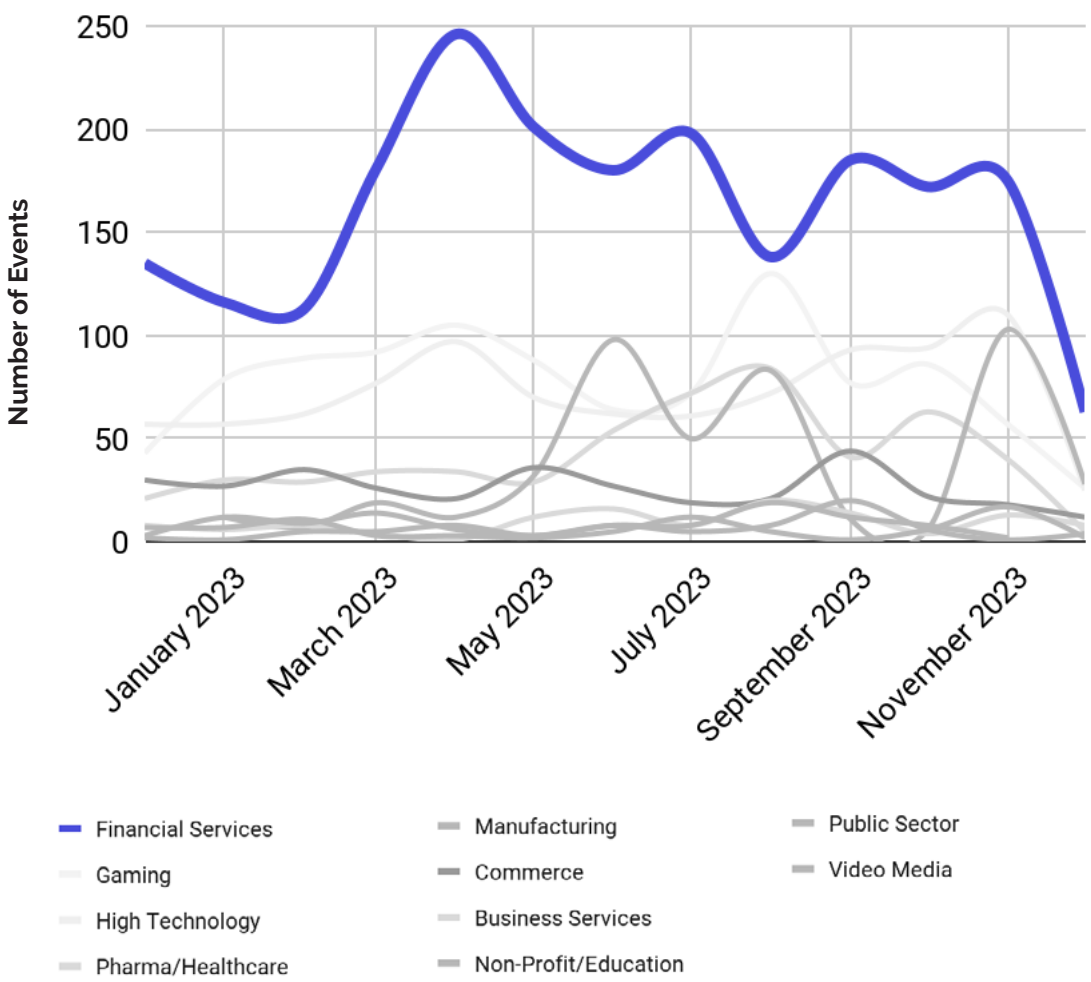



*Figure 2: Financial services saw the most attacks globally, representing 35% of attacks across all sectors. (Source: Akamai)*

## Regional Overview

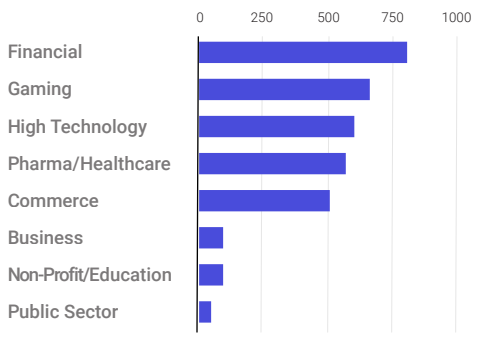
The financial services sector was the most targeted sector in the AMER and EMEA regions, though EMEA institutions were threat actors' preferred target by far: In EMEA, the financial services sector accounted for 66% of all DDoS attacks, compared to 28% in the AMER region. In the APAC region, financial services was the third most attacked sector, after commerce and gaming, and accounted for 11% of DDoS attacks.

Akamai analysis found that 51% of Layer 3 and Layer 4 DDoS events in 2023 were aimed at financial services organizations in EMEA. That shows a continuing "regional shift" trend, first observed in 2022, where the DDoS events in the EMEA region had increased by one-fifth and attacks on the financial services sector had increased by 73% since 2021.

The concentration of DDoS attacks in the EMEA region points to the use of DDoS as a tool of politics, hacktivism, and cyber warfare, specifically in relation to the Russia-Ukraine conflict.

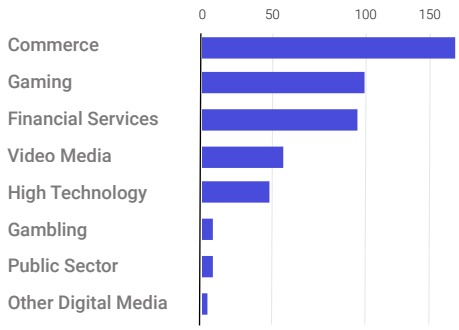
**Americas: Financial services represents 28% of DDoS attacks**

June 2023 - December 2023




**APAC: Financial services represents 11% of DDoS attacks**

June 2023 - December 2023




**EMEA: Financial services represents 66% of DDoS attacks**

June 2023 - December 2023

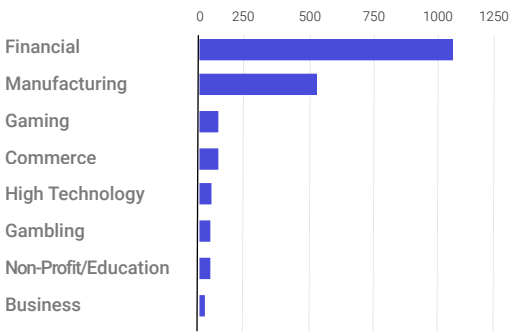



*Figure 3: Regional overview by sectors. (Source: Akamai)*

## Geopolitical Influence

Financial firms must ensure that their threat intelligence programs include geopolitical considerations and analyses, as the financial sector is likely to continue to be a hacktivist target in future geopolitical conflicts around the world.

Hacktivists are motivated by ideology and frequently attack powerful organizations, such as big commercial banks, public institutions, military facilities, and government agencies. Though they may lack advanced technical skills, hacktivists' DDoS attacks nonetheless pose a threat to service availability, though for relatively short periods.

The outbreak of the Israel-Hamas war increased the number of hacktivist DDoS attacks, but Russia's February 2022 invasion of Ukraine was a watershed moment, giving rise to a large number of new threat actors and escalating the activities of both sides' cyber-armies. That has had a significant impact on the cyberthreat landscape. Pro-Russian hacktivists, for instance, actively targeted the financial sector during 2023. In June 2023, KillNet announced it would conduct "massive" cyber attacks against the Western financial system. That campaign has not, apparently, had any significant result. However, hacktivists are known to use inflammatory rhetoric in an attempt to aggrandize non-impactful DDoS attacks as part of a disinformation campaign meant to make them appear stronger.

## Hacktivist Profile: NoName057(16)

NoName057(16) first arrived on the hacktivist scene shortly after Russia's invasion of Ukraine.

In August 2023, NoName recruited hackers with a campaign called "DDoSia," which offered rewards of up to 80,000 rubles paid via cryptocurrency. Standard hacktivist groups do not have the means to pay for DDoS attacks, making a financial tie to the Russian government likely. However, most of the DDoS attacks from NoName have been largely ineffectual and successfully mitigated.

The financial sector is a regular target of NoName. In 2023, they conducted daily attacks against critical infrastructure organizations, including large commercial banks, national banks, transportation, military facilities, and government agencies. The group's manifesto indicates a preference for targeting companies and organizations that express support for Ukraine or hold an "anti-Russia" stance. Hence, companies situated in NATO member countries or those supporting Ukraine should take proactive measures by acquiring DDoS protection services as a precautionary step against potential attacks from NoName.

## Hacktivist Profile: Anonymous Sudan

The group Anonymous Sudan emerged on Telegram in January 2023 and soon after pledged its loyalty to the pro-Russian hacktivist collective KillNet. Other than the group's public pledge to KillNet, the provenance of the group is unconfirmed, but security researchers have noted no actual ties to Sudan.

Though the actors say they share mutual interests with – rather than a connection to — Russia, the group's actions suggest pro-Kremlin sentiments. For example, Anonymous Sudan is the most prolific of pro-Russia hacktivist groups, its attacks have the greatest impact, and, according to researchers, its technical infrastructure would be cost prohibitive for a hacking collective, which points to a major financier, likely the Russian state.

The group has claimed responsibility for a number of high-profile DDoS attacks, including attacks against Sweden's critical infrastructure, the Israeli prime minister's website and Facebook accounts, Israel's national intelligence agency Mossad, several Emirati banks, Swedish Airlines, and various US hospitals. Since the outbreak of the conflict between Israel and Hamas, the group has begun to target pro-Israeli sites and organizations linked to the escalation of conflict in the Red Sea. The group has also claimed credit for conducting multiple website defacements and data leaks. Other major attacks claimed by the group include the compromise and temporary disarming of Israel's Iron Dome missile defense system and the June 2023 attack on Microsoft, which affected both Outlook and Azure.

## Hacktivist Profile: KillNet

Active since January 2022 and certainly one of the most prolific hacktivist groups throughout 2022, KillNet was a Russian hacktivist organization known for frequent, erratic, and publicity-focused DDoS attacks against US and Western financial, transportation, and government systems. On 5 June 2023, KillNet announced it had disbanded the group's existing structure, and in January 2024 announced it had reorganized into three different groups. Though widely regarded as more loud than effective, KillNet's membership included capable actors and a penchant for garnering support from like-minded actors. KillNet and Anonymous Sudan have demonstrated frequent connections with each other.

## More Than a Nuisance: Threat Actors' DDoS Use Cases

Though mature financial services organizations' defenses are typically robust, DDoS attacks are much more than a nuisance – they can disrupt millions of people if the attack successfully interrupts a software service on which any degree of global commerce depends. Moreover, DDoS attacks can be used as a smokescreen for other types of cyber attacks, such as part of an extortion scheme.

In fact, ransomware groups have incorporated DDoS events as part of their tactics, techniques, and procedures (TTPs). Triple extortion ransomware, also known as ransom DDoS (RDDoS), involves infiltrating businesses with ransomware, threatening to expose exfiltrated customer information if not paid, and disrupting business operations with a DDoS attack as extra pressure to force the victim to pay the ransom. RDDoS is becoming an increasingly disruptive form of cyber extortion and is gaining popularity as cybercriminals have been finding it lucrative. Ransomware groups such as BlackCat, AvosLocker, DarkSide, and Lazarus have been utilizing DDoS attacks in this way in their extortion schemes. However, FS-ISAC analysis finds members reporting a shift away from financially motivated DDOS extortion campaigns in 2023 to state-backed hacktivist groups.

A recent trend observed by DDoS researchers is the rise in threat actors' reconnaissance activity. This coincides with a sharp uptick in randomized and sophisticated DDoS attacks. The attacks appear deliberately engineered to try to overcome mitigation systems by imitating browser behavior. In many of these cases, the threat actors attempt to keep the attack-per-second rate low to avoid detection and hide in legitimate traffic.

Observers have also noticed hacktivists conducting DDoS attacks as a training method in the art of DDoS. Hacktivist groups and other attackers were observed to launch attacks against smaller targets as educational experiences to teach their crews how to launch attacks against larger and more important targets. Indeed, the KillNet hacking group admitted attacking the Italian public sector with the purpose of training and skills improvement.

## Evolving DDoS Attack Types in 2023

Though the threat landscape shows more DDoS attacks launched more often, it also indicates that threat actors are changing their DDoS attack types. The trend is toward shorter attack duration but bigger packet-per-second attack volume, and more attacks on applications/web pages. Specifically, increased malefactor activity directed at web infrastructure (attackers sent more requests per second in 2023 than in 2022), attempts on bandwidth meant to "clog internet pipes" (more bits per second sent), attacks on hardware/CPUs (more packets per second sent), and attacks on DNS infrastructure (more queries per second sent).

According to Akamai's insights, the most frequent DDoS attack vectors in 2023 were DNS flood (55%), followed by SYN flood, DNS reflection, and NTP reflection. FS-ISAC sees a variety of techniques, including the use of DNS reflection, GET flood, SYN flood, and Layer 3, Layer 4, and application Layer 7 attacks.

Further, observers noted more horizontal attacks in 2023. Horizontal attacks are simultaneous DDoS attacks aimed at multiple, unrelated targets rather than a single high-value victim. For example, adversaries might attack all the IP addresses associated with a particular organization, or attack a large number of active services or systems at once, following in-depth reconnaissance. Designed to distribute the attack, this DDoS approach maximizes the possibility of widespread disruption and makes mitigation more challenging.

Botnets are also becoming increasingly powerful. Since early 2023, hyper-volumetric DDoS attacks were more often associated with compromised virtual private servers (VPS) than with Internet of Things (IoT) devices. The new botnets use fewer devices, but each device is substantially stronger. For example, the VPS used by customers of cloud computing companies to create performance applications are 5,000 times stronger than IoT-based botnets.

## Notable DDoS Attacks in 2023

In 2023, several DDoS attacks were noteworthy, either for the target or the size of the attack.

**February 2023**

Akamai mitigated the largest DDoS attack ever launched against one of its customers based in the APAC region. Attack traffic peaked at 900.1 Gbps and 158.2 Mpps. The attack was intense and short-lived, with most attack traffic bursting during the peak minute of the attack.

**June 2023**

Microsoft's flagship office suite – including the Outlook email and OneDrive file-sharing apps – and cloud computing platform Azure were attacked with sporadic but serious service disruptions. The hacktivist group Anonymous Sudan claimed responsibility, saying it flooded the sites with junk traffic in DDoS attacks. According to Microsoft, this DDoS activity targeted Layer 7 rather than Layer 3 or 4.

**July 2023**

Akamai detected and mitigated the largest DDoS attack ever launched against a European customer, with globally distributed attack traffic peaking at 853.7 Gbps and 659.6 Mpps over 14 hours. The attack, which targeted a swath of customer IP addresses, formed the largest global horizontal attack ever mitigated by Akamai.

**September 2023**

One of America's biggest and most influential financial institutions was attacked by cybercriminals using a combination of ACK, PUSH, RESET, and SYN flood attack vectors, peaking at 633.7 Gbps and 55.1 Mpps. Akamai successfully detected and halted the attack within two minutes. Nevertheless, the attack was sharp, and disrupted the internal system operations and crippled the official website for a period of time. Shortly after, Anonymous Sudan claimed credit for the attack on its official Telegram page and disclosed its intention to shut the company's system down.

**November 2023**

OpenAI confirmed that a DDoS attack was behind "periodic outages" affecting ChatGPT and its developer tools. Hacktivist group Anonymous Sudan took credit for the alleged attack.

## DDoS HTTP/2 Rapid Reset Vulnerability

Early in 2023, security researchers discovered the existence of a unique zero-day vulnerability dubbed the "HTTP/2 Rapid Reset" attack (CVE-2023-44487).

This attack exploits a weakness in the HTTP/2 protocol to generate extremely hyper-volumetric DDoS attacks. This "never seen before" zero-day vulnerability attack leverages HTTP/2's stream cancellation feature by sending a request and immediately canceling it over and over. By automating the "request-cancel-request-cancel" pattern at scale, moderately-sized botnets can create a large volume of requests with the potential to overwhelm almost any server or application supporting HTTP/2. One record-breaking attack in August peaked just above 201 million requests per second.

Crucially, that attack involved a modestly-sized botnet, roughly 20,000 machines. That indicates the ability of a relatively small botnet to generate a substantial volume of requests with the potential to incapacitate any server or application supporting HTTP/2 – as every modern web server does. Because the attack abuses an underlying weakness in the HTTP/2 protocol, any vendor that has implemented HTTP/2 will be subject to the attack. That underscores the severity of this vulnerability for unprotected networks.

## Layer 7 and DNS Flood Attacks

In 2022, DDoS attacks primarily targeted Layer 3 and Layer 4. In 2023, Akamai observed an increase in Layer 7 and DNS attacks. Additionally, several financial services firms reported brief Layer 7 DDoS events targeting their infrastructure since the beginning of 2023. Affected organizations posit that these attacks indicate threat actors attempting to determine if corporate website functionality is degraded while they try to stay under the DDoS protection correlation time of five minutes before mitigation services kick in.

Application-layer DDoS attacks remain one of the most significant threats to financial services and applications. Unlike traditional Layer 3 or Layer 4 DDoS attacks, which aim to overwhelm network and transport layer infrastructure, application-layer DDoS attacks target specific application functionalities or the application server itself. Application-layer DDoS attacks could cause significant damage even with a relatively small amount of malicious traffic. Because they target application-level resources, such as CPU and memory, the targeted application or service may become slow or entirely unresponsive even if the network remains available. In addition, multi-vector attacks may also exploit specific vulnerabilities, such as software defects or misconfiguration, at the application layer. The evolution of IoT has made internet-connected devices more sophisticated and more difficult to defend.

## Pseudo-Random Subdomain Attacks (PRSDs)

NXDOMAIN attacks, increasingly prevalent, are characterized by their scale, duration, and frequency. These floods involve attackers targeting a domain with nonexistent randomly generated prefixed subdomain requests to subdomains that do not exist, prompting the targeted DNS servers to search for them and respond with an NXDOMAIN (non-existent domain) error message. Typically, internet service provider (ISP) domain servers cache frequently accessed subdomains, which aids in reducing the workload on authoritative DNS servers. However, by employing random subdomains, attackers ensure that each request reaches the origin server, thereby overwhelming the service.

# Mitigation

Although there is ample data on the number of blocked attacks, the type of attack vectors that were generated, newly discovered attack vectors, and how they were compromised or leveraged, there is still no comprehensive analysis of the attacked destinations and the techniques surrounding those behaviors. Although information is commonly shared on attack duration, size, and frequency, there is less focus on the techniques used to attack the destination. Understanding the TTPs used to attack the destination can help network operators and security experts better defend against such attacks. Organizations need to implement robust security

measures and regularly assess their networks and applications to prevent and mitigate the impacts of such an attack.

## Addressing Material Risk

DDoS attacks constitute differing levels of material risk. The definition of material risk is individual to each firm and must be decided upon by the CFO and leadership team. While a risk doesn't need to qualify as material to require mitigation controls, boards of directors should be involved in the decision. Further, financial services organizations' security teams should determine in partnership with the business when loss of access due to DDoS attack would qualify as a material risk.


It is worth noting that as the financial system is based on trust, brand and reputational impact are relevant to this discussion. While a DDoS attack may not meet specific monetary materiality metrics, the board may still deem the potential fallout of a DDoS attack beyond their cyber risk appetite.

Once the definition and thresholds of material risk have been defined, the organization should build out security controls, leverage services, or offset risk with insurance. This requires understanding the scope, speed, and complexity of current attack trends and methodologies. Then companies must validate their crisis management plan through exercises that test the technical capabilities, processes, and staff skills necessary to respond to a DDoS attack. Most financial services companies will find it sufficient to conduct these tests annually with their service provider as well as internally with table-top exercises to ensure the staff understands their responsibilities.

## DDoS Protection Services

There are many different as-a-service DDoS protection solutions on the market. These services detect attacks at an early stage, have the bandwidth to absorb the large-scale traffic of a DDoS attack, and can offer the resources necessary for effective mitigation. When choosing a DDoS mitigation service, the following questions are good reference points:

- What is the time-to-mitigation and application uptime guaranteed in the service agreement?
- What are the notification and audit rights stipulated in the agreement?
- Can the service provider's application work coincide with the organization's network environment?
- Does the protection fit the organization's business model, such as cloud/multicloud/hybrid environment, protection of the application layer, and protection for nontraditional web applications?

## Resilience

Financial services firms – particularly the more mature ones – tend to have strong DDoS protections in place. However, threat actors are continuously updating their tools and techniques, requiring ever more resources to ensure continuous uptime. Compared to other cyber events, DDoS attacks do not allow for any reaction time. Business continuity (BC) and disaster recovery (DR) plans are therefore crucial to financial services institutions' resilience. Minimizing technical debt, optimizing current tools and capabilities, and establishing repeatable processes that leverage automation can reduce the constant "fire drills" that sap staff energy and resources even as DDoS attacks against the financial sector increase.

However, that approach requires discipline and commitment to accomplish. It is therefore important to consider the impact an unplanned outage may have on users or customers and prepare for it by, for example, hosting on an alternate site on another ISP or content provider or by familiarizing staff with a different communication platform.

Business continuity teams should use the latest threat intelligence to inform plausible scenarios and conduct regular exercises with all relevant teams to build the muscle memory to respond to DDoS attacks, as well as validate and update playbooks. While the incident response playbook is key, organizations must also have a crisis management plan. Successful DDoS attacks can be very public, and discovery of an event should be immediately followed by communication with leadership and public relations, as well as consultation with compliance officers.

Vendor management procedures, in the case of third-party involvement, are also important. Some such issues are included in the Digital Operational Resilience Act (DORA) and similar regulations. CFOs, legal teams, and vendor management teams should determine which companies qualify as critical vendors and what contractual agreements are necessary, such as audit rights, cyber incident notification timelines, and clarity around resilience plans.

## Cyber Hygiene

Because cybersecurity involves active adversaries rather than potential accidental disruption, threat trends should be constantly assessed. No framework of best practices exists to prevent DDoS, but maintaining robust critical baseline cyber hygiene does help. DDoS attacks vary by type, including the exploitation of vulnerabilities and misconfiguration. It is therefore important to cover the basics, such as the following points:

- All software and apps need to be kept updated and patched. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats in general.
- All hardware, in particular older end-user devices, may need to be updated to prevent issues and maintain performance.
- Relevant vulnerabilities need to be analyzed to mitigate and remediate.
- Every new installation of devices and software should be documented in the inventory list.
- Unused devices should be identified, taken off the network, and properly disposed of.
- Admin-level access to devices and software should be limited strictly to those who need it. Other users should have limited capabilities to prevent unauthorized access.
- Password policies, enforcing complex passwords, and change cycle should be implemented.
- All data from the organization's devices and apps should be backed up to a secondary source segmented away from the primary network.

## Conclusion

DDoS attackers continue to use a variety of techniques to annoy, test, harass, and extort financial services companies. The sector will probably continue to see DDoS attacks, including high-volumetric attacks, from a variety of threat actors, chief among them politically motivated hacktivists and nation-states. Those cybercriminals will likely continue to make DDoS their attack of choice. With DDoS, they can create disruption without being named, thus avoiding legal accountability and/or possible retaliatory responses from other governments.

However, a key aspect of DDoS attacks is threat actors' inherent need for notoriety and attention. Threat groups often announce their attacks publicly, giving defenders the opportunity to cross-check the information with the cybercriminal's known TTPs, helping organizations both identify and increase their attribution confidence.

That is a significant advantage in the threat landscape. A greater advantage is a mitigation plan and cyber hygiene policies drafted in concert with organizational leaders, the business, and the cybersecurity team. Those practices protect institutions from the ever-present threat of DDoS attacks on the financial services sector. Such attacks, it seems, are likely to evolve, unlikely to stop, and can carry material risk. But they can be contained to nuisance status by well-prepared financial services cybersecurity organizations.

## Contact

www.fsisac.com
media@fsisac.com