FS-ISAC Akamai

The Evolution of DDoS: Return of the Hacktivists

January 2023

Contents

The Evolution of DDoS: Return of the Hacktivists

Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack employs multiple connected online devices, collectively known as a botnet, to overwhelm a target website with traffic, slowing or even disabling it altogether for legitimate users. DDoS attacks have been around for decades, but the recent increase in both volume and intensity is a rising concern to the financial sector.

Largely dormant for years, 2022 saw the return of DDoS attacks based on political motivations. Targets have consisted of government websites, private networks, education facilities, and critical infrastructure – including financial institutions - of entities that directly or indirectly have taken sides in the Russia-Ukraine war or other geopolitical tensions between China and Taiwan, as well as between the US, Israel, and Iran.

DDoS Attacks Targeting Financial Firms

⬆ 22%

DDoS Attacks Targeting Financial Firms in Europe

⬆ 73%

The volume of DDoS attacks targeting financial firms has increased by 22% since last year. This is especially true in Europe, where the attacks increased by 73%, and where financial services were the target of 50% of all DDoS assaults.

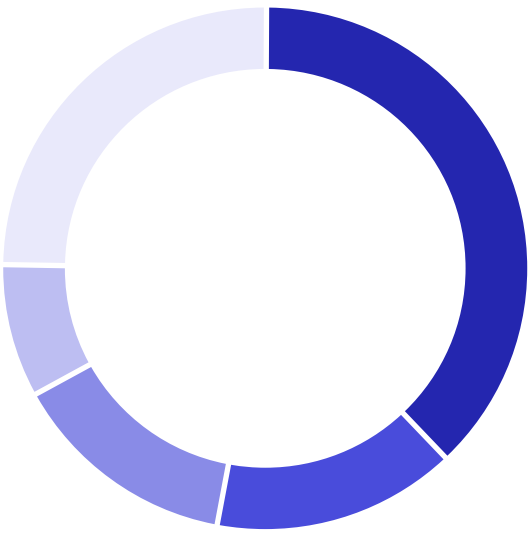
While this increase can largely be attributed to hacktivists, another key factor is the evolution of DDoS extortion attacks with financially motivated actors.

Finally, DDoS may also serve as a decoy, masking other more serious types of attacks such as malware or even espionage.

As such, what was once seen as a low-level nuisance increasingly poses key business risks, such as operational disruption and reputational damage, as well as compliance and supply chain risks.

Attack Types

Reported in the 2021 FS-ISAC Breach and Incident Survey



38% | DDoS

15% | Account Compromise

14% | Supply Chain

8% | Ransomware

25% | Other

DDoS for Hire: Denying Availability is Now Available to All

As with other types of cyber attacks, the DDoS supply chain is increasingly complex. Threat actors now specialize in specific skills and offer their services for hire using the as-a-Service (aaS) model. Would-be attackers with limited to no knowledge of how to perform a DDoS attack can now leverage these for-hire services and launch large-scale attacks using only an internet connection and a Dark Web browser. Some providers offer to conduct the attack on the client's behalf; others provide the client access to a panel with DDoS capabilities. There is no need for personal contact between the operators and their clients, which ensures a high degree of anonymity.

Record-breaking DDoS Attacks in 2022

Google Cloud
June 2022

Largest application layer attack

46M requests per second

European Organization
September 2022

Largest ever attack on European firm

704.8 mega-packets per second

Minecraft Server
October 2022

Largest DDoS attack in 2022

2.5 terabytes per second

The explosion of the Internet of Things (IoT) has been a boon to DDoS attackers, providing an endless army of poorly secured devices that they can requisition to serve as botnets. Some new techniques do not even require large amounts of bandwidth; they can send a small amount of traffic that capitalizes on network device vulnerabilities to amplify throughout the target system to achieve the same effect.

This commoditization combined with the easy availability of botnet infrastructure and amplification techniques is a toxic brew. In addition to greater volumes, DDoS attacks are increasing in intensity, requiring more resources to combat them. Although the peak volume of most attacks towards the financial sector remains under the 120 Gbps mark, there have been documented attacks with volumes up to 700 Gbps in 2022. The higher the intensity, the more likely the attack will overwhelm firms' mitigation measures. Thus far, these high intensity attacks have been minimally successful; however, higher intensity attacks could have impact. Attacks of much lower intensity can also be successful if mitigation does not kick in in time to alleviate the impact.

The speed at which these attacks reach their peak and the duration of them staying at that peak is also on the rise, giving firms less time to mitigate.

Further, there is now a range of attack types beyond the simple volumetric clogging of internet pipes. Attacks can also target hardware, DNS infrastructure, and even web servers, giving threat actors more means to achieve their ends. According to Akamai data, in 2010 the top five DDoS attack vectors mounted up to 90% of all attacks. In 2022, the top five vectors only account for 55% of all attacks. This indicates the threat landscape is maturing and becoming more varied, complex, and sophisticated. Some vectors dominate for a short period until mitigation measures catch up, while others stand the test of time.

With the crisis between Ukraine and Russia, numerous DDoS incidents targeting Ukrainian and neighboring country banks, businesses, and government websites continue to be reported to FS-ISAC. However, Ukrainian entities are far from the only targets.

Taking a Cue from Ransomware's Success

The financial sector is better protected than many other industries because of a long legacy of regulation and resulting robust cyber posture, which includes DDoS mitigation strategies. However, financially motivated DDoS actors are increasingly adding extortion to their tactics, which is not necessarily covered by existing protections. As Akamai has noted, DDoS attacks increasingly now include a ransom note demanding payment to cease the attacks.

In one DDoS extortion campaign focused on financial institutions and cryptocurrency companies that started in 2020 and has affected dozens of FS-ISAC members around the globe, threat actors claim to hail from famous and successful threat groups including Russian Cozy Bear and Fancy Bear, North Korean-affiliated Lazarus Group, or a combination – "Fancy Lazarus." They seem to be invoking the "brand-name" groups to give their campaigns gravity and credibility. However, it is unlikely these sophisticated groups are involved, given that the attacks tend to leverage vectors that are easily mitigated. Although these actors are likely less capable than the nation-state APT groups they name, the demonstrative DDoS activity associated with this type of attack appears to be more advanced than similar campaigns in 2017 and 2019, occurring at growing volumes and employing multiple vectors.

Other DDoS extortion campaigns claim to be from known ransomware operators such as REvil and Conti. However, similar to "Fancy Lazarus," analysis proves that the named threat groups are unlikely to be related to the campaigns. While most FS-ISAC members affected by these campaigns reported no or limited impact, the attacks could present mitigation challenges for some firms.

▶ DDoS Actor Profile: Killnet

The *Killnet* cybercrime syndicate first appeared in January 2022 while advertising its DDoS-for-hire services on underground forums. During the Russian invasion of Ukraine, *Killnet* pledged its allegiance to the Russian government and declared hostility against anyone opposed to the regime. This was followed by targeted attacks against state- and privately-owned websites located in countries considered to be unfriendly to Russia, such as those who imposed sanctions for Russia's invasion of Ukraine. In 2022, targets have included NATO member countries (March–April), government and private websites belonging to Romania (April), Italy (May), Lithuania (June), Norway (June), and Japan (September); and multiple US-based sites, such as the US Treasury, a financial institution, and numerous airports (October and November).

Throughout 2022, *Killnet* was one of the most active hacktivist organizations and has proven that it can have an impact on services all over the world. Instead of creating serious harm or generating substantial financial benefit, *Killnet* seems to be more concerned with notoriety. It is highly possible that *Killnet* agents will continue to promote a pro-Kremlin narrative and attack entities that disagree. *Killnet's* new commander, BlackSide, is reported to be an expert at running phishing, ransomware, and crypto-theft assaults. This may indicate that the hacktivist group is looking to expand and improve its operational capabilities for upcoming campaigns.

DDoS as Decoy

Importantly, DDoS can also serve as a cover for other, potentially more damaging cyber activities such as infiltration of systems and exfiltration of data, and malware installation. Although the majority of DDoS attacks, in particular within the financial sector, do not actually cause much downtime due to the array of standard defensive measures applied to counter their effects, they still can be highly disruptive, requiring shifts in security resources and slowing down operations. The distraction caused to the victim organization can serve as a smokescreen, which makes it easier to achieve or hide other types of attacks. One example of such tactics occurred

more than a decade ago, when the Dirt Jumper botnet aided decoy DDoS attacks against banks.

This means that when cybersecurity teams encounter DDoS, they must also instantly be on the alert for other types of attacks, putting extra strain on already limited resources.

From Nuisance to Key Business Risk

The evolution of DDoS means that financial firms must update their risk profiles and mitigation measures accordingly. Far from a low-level annoyance, DDoS should increasingly be considered a key cyber defense challenge with the following corresponding risks.

Financial Services Comparative Industry Ranking for Attacks

vs. other industries, i.e. technology, e-commerce, media, etc.

#1 Phishing

#2 DDoS

#3 App and API

(Source: Akamai)

Operational

The most obvious impact is to business operations should customer-facing or other websites be disrupted. While financial services firms tend to have DDoS mitigation strategies in place, the increasing sophistication of DDoS attackers should not be underestimated. Mitigation strategies need to evolve constantly to keep up with the increasing variety, volume, and intensity of attacks, which could require significantly more resources over time.

Further, with the large-scale move to remote work, many organizations now face potentially serious operational impact if workers can't reach work resources remotely. A targeted attack designed to cause outage or service degradation against a VPN site, authentication service, or other remote access infrastructure may bring business to a halt in a unit relying heavily on work-from-home staff.

Insider Threat

In FS-ISAC's *2021 Breach and Incident Survey*, a case was reported of an eBanking user sending a large number of requests that caused disruption in the service. In that case it was likely a compromised customer's account, however the attack traffic managed to evade all the controls put in place against DDoS because the traffic was authenticated. Internal DDoS attacks, whether due to tool misconfiguration or malicious intent, should be taken into consideration when designing DDoS controls.

Supply Chain

As more services are moved to the cloud or contracted in an aaS (as-a-Service) model, those services will depend on other supply chain components. Service disruptions anywhere in the supply chain can have a serious impact on an organization's operations. In FS-ISAC's *2021 Breach and Incident Survey*, 11% of the reported DDoS attacks did not target the financial institution itself, but rather a third- or fourth-party provider.

Our increasingly remote workforce is another important consideration here. Loss or degradation of internet, cellular connectivity, and/or telephony could mean workers cannot access the resources required to do their work. Relying solely on workers' own communications providers means employers no longer control these channels and therefore cannot put adequate defenses in place.

Reputational

Threat actors focused on notoriety often post screenshots on social media of unavailable websites as trophies for their work. Even if a site is down for a few seconds and has no operational disruption, the evidence that threat actors were at all successful could damage trust in the sector's cyber defenses.

Compliance

In August 2020, a DDoS attack brought the New Zealand Stock Exchange (NZX) website offline. The NZX website is where market updates are published for public consumption. Market update availability is a regulatory condition for trade. Therefore, when the website went offline and market updates were

no longer available, trading could not continue. Even though the trading platform was not under attack and remained unaffected, the NZX was in breach of regulation. When considering DDoS controls, every service needs to be evaluated regarding its criticality level and how an outage may affect other services technologically or procedurally linked to them. The unavailability of a service may change the overall risk stance in regulatory compliance or contractual commitments.

Mitigation Strategies

Given the ubiquity of the DDoS threat and the mitigation challenges, firms may consider cyber insurance as one way to address the risk from DDoS. However, as cyber attacks are increasing, improving, and becoming cheaper and simpler to carry out, cyber insurance policies are becoming more limited and more costly. Relying on cyber insurance is not a mitigation strategy.

While by no means exhaustive, the following guidance is a minimum baseline set of practices firms should employ when considering upgrading DDoS defenses.

DDoS Protection Services

Given the increase in variety, volume, and intensity of DDoS attacks, on-site mitigation is becoming a challenge even for the largest, most mature organizations. DDoS protection services can detect attacks at early stages and have the bandwidth to absorb large-scale traffic, as well as the resources necessary for effective mitigation. Key considerations include:

- Time to mitigation and application uptime guaranteed in the service agreement
- Notification and audit rights stipulated in the agreement
- Whether the service provider's application work coincides with your network environment
- Ensuring the protection covers your specific environment, including cloud/multi-cloud/hybrid, application layer, VoiP, etc.

Network Best Practices

Inventory

One of the most important things an organization can do is keep records of all its hardware and software. A proper inventory list is a prerequisite for creating a complete network architecture map. The inventory and network map are used as guides for putting security policies in place, setting up hardware, prioritizing critical assets, and meeting cyber hygiene goals. Inventories should include:

- **Hardware:** connected devices such as printers, servers, and mobile devices that are used on the organization's network as well as end user devices
- **Software:** all software that is installed directly onto the organization's devices, including software-as-a-service (SaaS) and mobile applications
- **IP subnets:** a list of all IP spaces used to ensure DDoS and access mitigation controls are in place for critical access nodes

Cyber Hygiene Policy

Cyber hygiene practices should be documented into a standard policy to be followed by all who access the network, and tasks should be scheduled regularly to ensure continuous coverage. Examples include:

- All software and apps are kept updated and patched to mitigate vulnerabilities that may be exploited for DDoS attacks.
- All hardware, and in particular older end user devices, are updated to prevent issues and maintain performance.
- Relevant vulnerabilities are analyzed for mitigation and remediation.
- Every new install of devices and software is documented in the inventory list.
- Unused devices are identified, taken off the network and properly disposed of.
- Admin-level access to devices and software is limited strictly to those who need it. Other users have limited capabilities to prevent unauthorized access.
- Password policies, enforcing complex passwords, and a regular change cycle are implemented.
- All data from the organization's devices and apps is backed up to a secondary source segmented away from the primary network.

Exercises

Firms should use the latest threat intelligence to inform plausible scenarios and conduct regular exercises with all relevant teams to ensure firms continually build the muscle memory to respond to DDoS attacks, as well as validate and update playbooks to account for evolving threat actor tools, techniques, and procedures.

Crisis Management

Having an incident response playbook is key, but firms must also maintain a crisis management plan to leverage a coordinated response. DDoS attacks are usually very public, so there is a need to immediately inform stakeholders, including leadership, communications/public relations, compliance (who may need to notify regulators), and vendor management in the case of third-party involvement. The objective is to avoid having regulators or the press call an employee who is unaware of the incident. This requires identifying predetermined levels of impact to initiate the plan and a RACI (responsible, accountable, consulted, and informed) response so that each team member knows their role and who to contact.

If mitigation efforts prove insufficient, consider the impact on users or customers and be prepared to pivot. One best practice is hosting an alternate site on another ISP or content provider ahead of time, then redirecting traffic there in times of crisis. It can positively impact users' confidence and help mitigate the reputational damage from the sudden, unexplained unavailability of services.

Contact

www.fsisac.com
media@fsisac.com