Economic Commentary

Distributed denial-of-service attacks in the financial sector

Gabriella Ström

NR 10 2025, 6 November

Summary

In recent years, distributed denial-of-service (DDoS) attacks have become both more numerous and more complex. In Sweden, several serious attacks have targeted essential digital infrastructure, including financial services. The attacks on financial actors have led to short-term problems in accessing some services. However, if the threat to Sweden were to escalate, there is a risk of more advanced attacks, which could potentially have more far-reaching consequences. This could reduce confidence in the financial system or, in the longer term, impair the ability to make payments. Preventing DDoS attacks and minimising their impact requires action at several levels of society. This includes effective cooperation between the private and public sectors.

Author: Gabriella Ström, who works in the Financial Stability Division, Infrastructure and Cyber Division.[1]

Distributed denial-of-service attacks can affect the availability of financial services

The financial sector is largely digitalised and tightly interconnected, both financially and digitally. For things to work smoothly, services need to be available, and stakeholders need to have trust and confidence in the system. However, financial institutions risk being subjected to cyber-attacks, and DDoS attacks are one example of this. During a DDoS attack, the availability of a service is affected by the attacker sending traffic to the chosen target, thereby consuming a significant portion of a limited resource, such as the capacity of a server to respond to calls or the ability of a network to handle a lot of traffic at the same time. As a consequence, legitimate traffic to the server, service or network fails to arrive because the target or its surrounding infrastructure is overwhelmed with a flood of internet traffic whose sole purpose is to block other traffic.

[1] Thank you to Olof Sandstedt, Johanna Stenkula von Rosén, Kristian Jönsson, Björn Segendorff, Joacim Häggmark and Emanuel Hedestig.

Diagram 1:

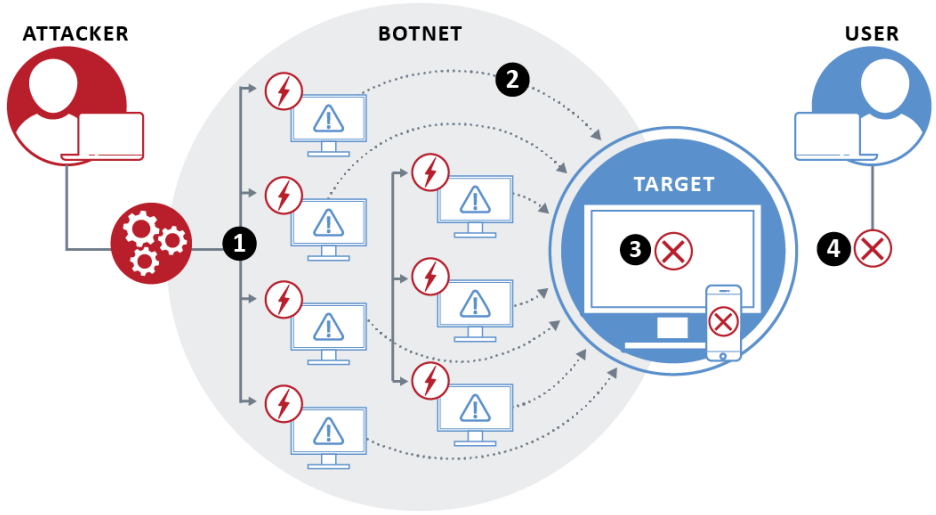

Diagram 1: (1) A network of computers is infected with malware and can be remotely controlled by an attacker. (2) At a given signal, all devices simultaneously send traffic towards a target, e.g. a website. (3) The huge volume of traffic overwhelms the target's capacity. (4) The service becomes inaccessible to ordinary users.

Recurrent disruptions can give the impression that the system is unstable, which in turn can lead to a loss of confidence. Such scenarios can be detrimental to the financial system, as trust is one of the basic prerequisites for the smooth functioning of the financial system. For trust to be maintained, data must be accurate and available to the right people at the right time.

Several serious attacks against Swedish financial institutions

In autumn 2024 and spring 2025, several Swedish banks and financial infrastructure operators were targeted by a number of serious DDoS attacks. The attacks caused disruption to the services of several of the affected operators. For example, it was not possible to access banking services via mobile apps or to make Swish payments.

One of those affected was the Financial ID technology BID AB's BankID service. The service is a key component of several important public services, including financial services. This is because it provides access to various services by providing identification and signature. With so many services using BankID, the attack caused problems for several different organisations at the same time. This was particularly noticeable among financial institutions, with several of them reporting incidents of BankID being overloaded. The attacks demonstrated how attacks against system-critical components have a wider impact.

By contrast, the consequences of the attacks on Swedish financial actors in 2024 and 2025 were only short-term disruptions for a limited period. As a result, the interruptions had no direct impact on financial stability. Nor have the attacks had an impact

on the capital markets or left a significant mark on the balance sheets and profit and loss accounts of the affected operators.

Still, it is important to be able to deal with attacks in a resilient way to ensure that they do not damage trust. The institutions affected by DDoS attacks have had to allocate some resources to successfully manage and mitigate the effects of the attacks. The resources required have been significant, both during the attacks and in the build-up to dealing with any future attacks.

Recovery from attacks is usually rapid

The explanation for the fact that DDoS attacks usually do not have a major direct financial impact lies partly in the method of attack. A system subjected to a DDoS attack is unavailable for the duration of the attack. If the attacker pauses or stops the attack, its effects also disappear. The target can usually recover as soon as the attack is over without any residual impact on the system.

Ransomware attacks function differently. The attacker then encrypts the data contained in the system, making it inaccessible. Subsequently, the victim is often required to pay a ransom to obtain a decryption key, with which the data can be accessed again. However, there is no guarantee that the data decrypted is reliable and accurate. In the case of a ransomware attack, both the impact and the recovery time are significantly longer. The system remains inaccessible until it has been isolated, examined and the encrypted data replaced, if possible, by data from backups.

Greater number of and more sophisticated distributed denial-of-service attacks

DDoS attacks are not a new phenomenon. However, the attacks are more sophisticated today than in the past. This is because they are largely precision-oriented and designed to maximise impact. In addition, the attacks have become more widespread.

The European cybersecurity authority ENISA reports that DDoS attacks are one of the primary cyber threats to the financial sector in Europe. Moreover, the National Cyber Security Centre's (NCSC) report *Överbelastningsangrepp mot kritisk infrastruktur i Norden och Baltikum hösten 2024* (*Critical infrastructure denial-of-service attacks in the Nordic and Baltic countries in autumn 2024)* shows that almost 30 per cent of the DDoS attacks observed in the Swedish IP space in September and October 2024 were directed at critical infrastructure. This includes government agencies, academic institutions and the telecom and finance sectors. In addition, over the past two years, DDoS attacks have increased in volume and become more frequent.

Diagram 2:

Figure 5: Threats observed in the European finance sector (January 2023 to June 2024)

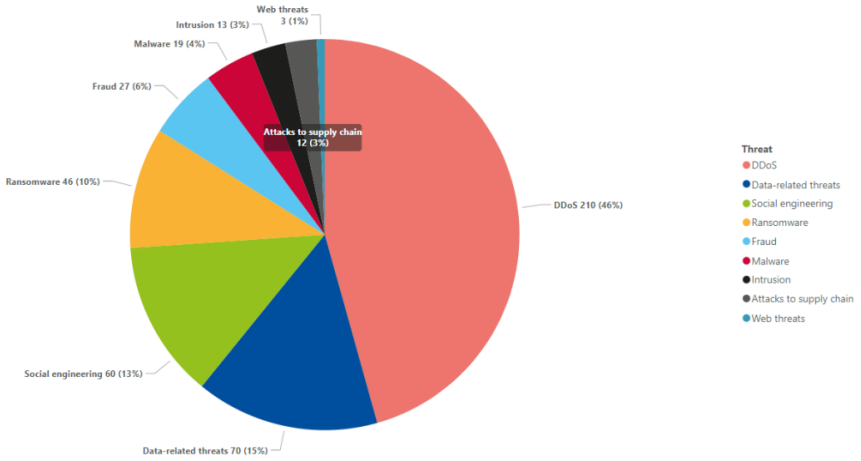

Diagram 2: The types of threat aimed at the European financial sector were as follows. The analysis is based on incidents reported to ENISA. As one incident can belong to several threat categories, the total percentage in the diagram exceeds 100%. (Source: ENISA, 2024).

Although the attacks of recent years have not had a significant impact on the financial sector and its services, it is not possible at this stage to predict what will happen in the future. The attacks could increase further in complexity, volume and frequency, leading to a greater number of disruptions and more widespread consequences.

It is also possible that tailored DDoS attacks against certain operators, with the aim of blocking all payment options, could have a noticeable impact. In a scenario where one or more institutions are overwhelmed at the same time, it is conceivable that the ability to make payments would be disrupted in a more fundamental manner.

Distributed denial-of-service attacks as a service

DDoS attacks can be carried out from the attacker's own computer or from computers otherwise at the attacker's disposal. The attacks can have a greater impact by using multiple hacked computer systems as sources of attack traffic. The devices utilised can be computers and other networked resources, such as IoT devices[2]. Moreover, the standard of security in such devices is usually lower than in a conventional computer.

The individual units are called bots, and a group of such bots is called a botnet. Once a botnet is established, the attacker can direct an attack by sending remote instructions to each bot and, as each bot is a legitimate internet-connected device, it can be difficult to distinguish the attack traffic from regular traffic.

[2] The Internet-of-things (IoT) means that everyday objects such as sensors, lights or refrigerators are connected to the internet to collect data or be controlled remotely.

Today, botnets and other necessary technical means are provided as part of a service offerings by various cybercrime networks. This is usually referred to as DDoS-as-a-service, which can be likened to a business model. The business model can vary from case to case. Some providers offer to perform the attack for the client, while others give the client access to a control panel with DDoS functions. This means that no in-depth technical expertise is required to carry out a DDoS attack. It also usually does not require any personal contact between provider and client, allowing the threat actor behind an attack to stay hidden and remain anonymous.

An example of such a delivery is the GorillaBot botnet, see Diagram 3. The botnet has, among other things, been used in several attacks against Swedish financial organisations.

Diagram 3:

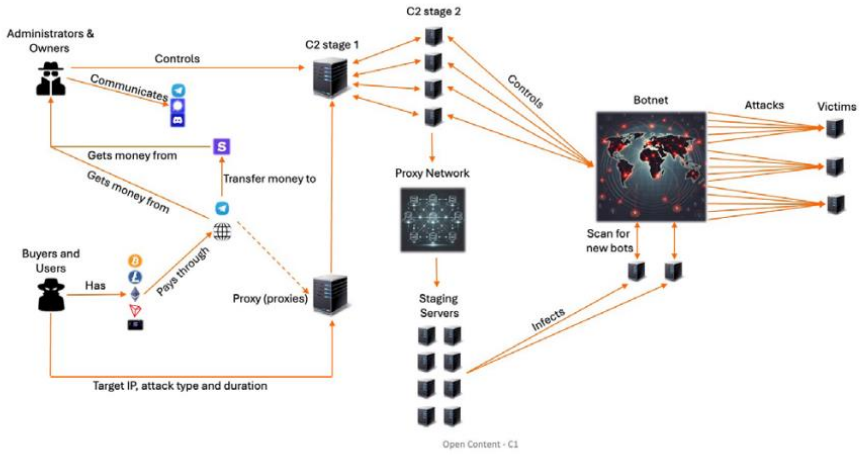

Diagram 3: An overview of the infrastructure behind the GorillaBot botnet (Source: NCSC, 2025).

Large and disruptive attacks have thus become more common. This is partly due to the large number of DDoS-as-a-service offerings and the fact that it is so easy to build a botnet, given that our lives are characterised by connected devices with low security.

The threat actors behind the attacks

The threat actors carrying out cyber-attacks against Sweden are mainly criminal, ideologically motivated and state actors. As anyone can use the same infrastructure to carry out a cyber-attack, it is often difficult to determine who is behind an attack. In some cases, it is clearer who is behind it, such as the pro-Russian group NoName 057(16). In other cases, the threat actor uses the possibility of anonymity, making it difficult to attribute an attack to a specific actor.

When it is difficult to identify the threat actors, it is also more difficult to understand the motives behind the attacks. However, patterns have been observed which suggest

that there are geopolitical motivations behind the DDoS attacks of recent years. In addition, the NCSC points out that the attacks in 2024 were likely fuelled by geopolitical conflicts and ideological motivations, so-called hacktivism, as well as the emergence of more sophisticated approaches. Similarly, ENISA reports that hacktivist-led DDoS attacks clearly dominate the threat landscape against financial actors in Europe.

Stopping distributed denial-of-service attacks and services

The wave of DDoS attacks that swept across Sweden in the autumn of 2024 and spring of 2025 provoked a heightened awareness and a sharpened approach to the method of attack. The escalating threat environment led Swedish financial sector actors to develop additional defences to build resilience against these attacks. However, it is uncertain how advanced DDoS attacks will develop over time. Maintaining resilience to them requires a proactive approach to adjusting and developing protection. This is to be able to robustly deal with an increasing number and complexity of attacks.

The scale of DDoS as-a-service offerings has led to increased efforts to try to limit the problem. Law enforcement agencies are cooperating internationally in efforts to dismantle overload service providers and botnets (Europol, n.d.).

In addition, the Cyber Resilience Act (EU, 2019) will begin to apply from 2027. The new regulation aims to enhance the security of connected devices, such as IoT devices, by introducing security requirements for hardware and software. This can make the devices more difficult to hack and therefore less easily exploitable by botnets. Individuals can also contribute to making their devices more difficult to hack. This is done by regularly updating software, not using the same login and password for multiple purposes, and by changing factory-set passwords when a device is installed.

Leadership and cooperation needed

Moreover, action is needed at several different levels. In addition to improved safeguards at the organisational level, collaboration at the societal level is also needed to counteract and limit the impact of cyber-attacks in the financial sector. The Riksbank currently participates in both international and national cooperation forums. One example is the NCSC finansforum. The forum aims to strengthen cybersecurity and thus financial stability by promoting information sharing between the private and public sectors. Since 2023, the Riksbank has also been a member of the Nordic Financial Computer Emergency Response Team (NFCERT). This organisation supports the Nordic financial sector in defending itself against cyber-attacks, for example by sharing threat intelligence.

Maintaining resilience requires that existing forms of cooperation are continuously developed, but also that new ones are initiated. Therefore, it has been proposed that the Riksbank should lead a new crisis management function (Riksbank, 2025). The function's mission is to coordinate the response to serious operational disturbances in the financial sector. In addition to the Riksbank, it is proposed that

Finansinspektionen (the Swedish Financial Supervisory Authority), the Swedish National Debt Office and certain companies in the financial sector be included in the function, together with other actors whose knowledge or resources are of importance to the function's work. The Riksbank is in favour of the task of leading such a function, as it could strengthen cooperation in the event of serious disruptions.

References

ENISA. (2024). Threat Landscape: Finance Sector. February 2024. European Union Agency for Cybersecurity.

NCSC. (2024). Cyber-attacks against critical infrastructure in the Nordic and Baltic countries in autumn 2024. National Cybersecurity Centre.

ENISA. (2025). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity.

Europol. (n.d.). *Cyberattacks*. Europol. Retrieved from https://www.europol.europa.eu/crime-areas/cyber-attacks (accessed 16 October 2025).

EU (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Official Journal of the European Union, L 151, 7 June 2019, pp. 15-69. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj

The Riksbank. (2025). Riksbank supports proposal for new financial sector crisis management function. Retrieved 13 October 2025 from https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2025/riksbank-supports-proposal-for-new-financial-sector-crisis-management-function/

SVERIGES RIKSBANK
Tel +46 8 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUCTION SVERIGES RIKSBANK