Recorded Future®

TRUESEC

Threats to the Swedish Financial Sector in 2021

By Recorded Future and Truesec

Executive Summary

Although Sweden's finance sector has fewer widely reported cyberattacks than many of its European neighbors or other countries internationally, it has faced numerous cyberattacks in 2021, many of which have been successful. Additionally, Sweden's population's preference for debit over credit has translated to greater criminal attention to acquiring and selling Swedish debit card data. Based on a review of attacks against this sector by Recorded Future and Truesec, we believe that DDoS attacks and ransomware attacks are major threats to this sector. Organizations in the Swedish finance sector should confirm that they are positioned to withstand both types of threats.

Key Judgments

- Compared to other European countries, Sweden and the other Nordic countries have featured much less prominently in the news as locations for victims of cyberattacks. While cybercrime in Sweden involves many malicious activities, some methods are more prevalent, including ransomware, business email compromise, and distributed denial-of-service (DDoS) attacks; these attacks are often facilitated by phishing and vulnerability exploitation.
- In most cases, criminals on dark web and underground forums and marketplaces prefer to target financial organizations' customers rather than the organizations themselves, which holds true for the Swedish market. Availability of victims was very likely the key factor for determining criminal discussion of Swedish financial organizations in 2021, with larger banks like Swedbank or Nordea receiving vastly more attention than smaller banks in the region. Furthermore, criminals were far more likely to sell debit card data rather than credit card data associated with Swedish banks, almost certainly reflecting the country's preference for debit over credit.
- The most prominent example of a Swedish finance victim of ransomware is likely that of Swedish finance broker Aktieinvest, which in October 2021 became a victim of the LockBit 2.0 ransomware operators, making them the second Swedish victim to appear on LockBit's extortion site after plastic parts manufacturer Prototal Industries.
- DDoS attacks have recently emerged as a major threat against financial organizations, including those in Sweden. The strength of DDoS attacks has grown exponentially in the last decade, and criminals continue to sell DDoS attacks as a service inexpensively. Per Truesec, while DDoS ransom is only a small portion of all cybercrime attacks, they represent nearly all known successful attacks against financial institutions in Sweden.
- The successful ransomware attack against Aktieinvest shows that the rapid growth of ransomware means that the threat to medium-sized fintech companies, below the big banks, may now be increasing. As the number of threat actors increases, they cast a wider net to find new victims. While the Klarna breach resulted from a bug and not a cyberattack, it also indicates that newer fintech companies, often heavily reliant on the internet, may not always have the same level of maturity in their cybersecurity.

Table of Contents

Threat Analysis

Major Trends in Cyberattacks against Sweden

Sweden: A Less Targeted Target?

Public reports of cyberattacks against organizations in Sweden, particularly in the Swedish finance sector, have been few and far between in 2021. The few major examples of Swedish cyberattack victims in the last year include the fintech company Klarna, which faced a data breach and subsequent regulatory investigation in Q2; supermarket chain Coop, which was affected by the ransomware attack on managed services provider Kaseya in early Q3; and financial services company Aktieinvest, which was hit with a ransomware attack in early Q4, purportedly from the prolific ransomware LockBit 2.0.

Compared to other European countries, Sweden and the other Nordic countries have featured much less prominently in the news as locations for victims of cyberattacks or threat campaigns. In a review of Recorded Future platform references to cyberattacks against victims in certain countries (which takes into account a vast number of sources from mainstream news to dark web forums to security vendor reports), the ratio of references to the Nordic countries and references to other European countries like Germany or France was roughly 20:1.

- In a specific example, per open source reports, banking trojans have largely left Sweden and the Nordic region unaffected compared to the rest of Europe. While at least one banking trojan has affected a Sweden-related bank (Nordea) in the past 2 years, it mainly hit customers in Finland. More recently observed banking trojans like Teabot and Eventbot have tended to affect finance customers in Western and Southern Europe.
- More dangerous cybercriminal and APT groups also have seemed to focus less on Sweden than other European countries, per open source reports. In late 2020, Sweden was listed by Kaspersky as a target of the Deathstalker "hack-for-hire" group, but only per a map of victim countries; an earlier report by Kaspersky about Deathstalker activities mentioned several victim countries by name, none of them Sweden.

Additionally, per an analysis of criminal discussion of Swedish financial institutions on dark web and underground forum sources, this sector is the target of much less criminal interest and fewer attacks than financial organizations in other countries. Compared to other European countries, including the United Kingdom, France, and Germany, Sweden is less of a target for online sales of credit card data. Within the Nordic countries, we have seen the most criminal attention to clients of major Swedish banks like Nordea, but past these, there is little to no criminal discussion.

A final comparison is the number of typsoquat domains registered to imitate finance organizations in certain countries. A review of such typosquats in the first half of 2021 found that Swedbank, for example, was the target of fewer apparent typosquat attempts than major banks in other countries such as HSBC, BNP Paribas, or Bank of America (with Bank of America outpacing Swedbank in this category by roughly 6:1).

Part of these trends is very likely related to population as a measure of opportunity for criminals: Sweden's population of 10 million is drastically dwarfed by the United States' 330 million, and is much less target-rich than other European countries like Germany (83 million) or France (67 million). Part of these trends is also likely related to cultural factors. For example, as reported in January 2021, a study from the European Commission found that Swedes were the most likely (at 92% of respondents) of any European country to contact police if they fell victim to banking fraud. Transparency about cyberattacks goes a long way toward highlighting, and thereby mitigating, tactics in use by cyberattack campaigns.

The threat landscape for the Swedish finance sector is less obviously affected by cyber threats than other industries worldwide. In large part, we consider that this is due to the finance sector's necessary hardening of cyber defenses in the last few decades in the face of persistent criminal interest in compromising banks' and banking clients' accounts. As a very highly digitized country, Sweden has also needed to adopt good cyber defense measures in many different sectors, contributing to security overall. However, this is likely a singular moment for the sector: while the landscape is relatively quiet now, improvements in security worldwide will almost certainly drive criminal ability to the point where the traditional banking sector in Sweden is again as much at risk as others in the European region.

The Swedish finance sector is also subject to the EU General Data Protection Regulation (GDPR), which states that any organization that is negligent in protecting personal data may be subject to penalties, including severe fines. Organized cybercrime syndicates are very aware of these rules, which they use to pressure their victims into paying larger ransoms. In addition to demanding ransom for decrypting data affected by ransomware, many cybercrime groups steal sensitive data and use it for additional extortion. This also has the unfortunate effect that victims of cybercrime often try to hide this to avoid possible GDPR fines, which gives more leverage to the criminals.

Under the Surface, Sweden Faces Multiple Cyber Threats

Despite the relatively minimal public reporting of cyberattacks or lower criminal discussion of potential victims, Sweden is not immune to many forms of cyber threats. While cybercrime in Sweden involves many malicious activities, some methods are more prevalent than others. The data below is based on data from the Truesec Incident Response team during the first 6 months of 2021. The data is therefore based on successful, or at least partially successful, attacks.

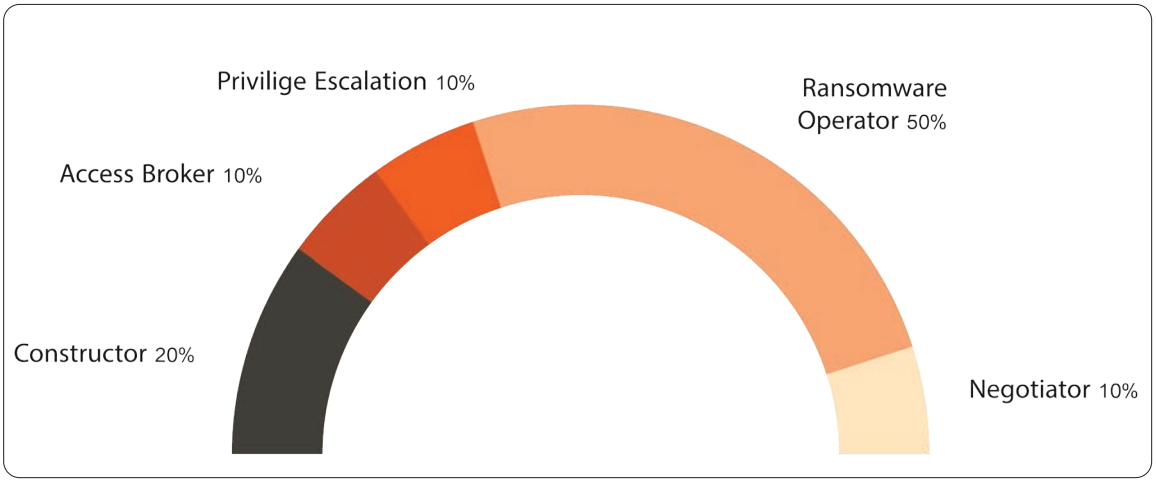

Figure 1: Attack types against victims of cyberattacks in Sweden, January-June 2021 (Source: Truesec)

Attack Types

Overall, ransomware attacks have been the most common form of financially motivated cyberattacks in recent years. Access harvesting is only a means to obtain access to a network for further attacks. With the increased diversification in cybercrime, however, some groups now specialize in obtaining access to networks and then selling the access to other groups. Most of those attacks would likely have resulted in ransomware or some other form of attack if unchecked.

Ransomware attacks often are paired with data leak ransom. Ransomware groups also steal data from the victim's network and then blackmail them by threatening to release sensitive corporate information on the internet, an extortion technique called "double ransom". In the first 6 months of 2021 about 70% of all ransomware attacks also involve data leak ransom.

Ransomware groups try to maximize the pressure on their victims. Many groups add DDoS attacks and even threatening phone calls to key personnel to frighten victims into paying the ransom. Other groups threaten to immediately leak sensitive data if the victim tries to contact law enforcement or cybersecurity professionals in an effort to isolate the victim.

Another important development is that some ransomware gangs now openly try to solicit insiders to deploy the ransomware on networks they have access to. If this method is successful, it is highly likely to be copied by other groups.

An important driver in the increase in ransomware attacks is unregulated cryptocurrencies like Bitcoin. The lack of regulation allows cybercriminals to acquire extortion money without a trace. The ransoms demanded in these attacks, often based on public information about the organization's turnover, has increased dramatically to over 290 million SEK in some cases.

Business Email Compromise (BEC) is a simple but effective form of transaction hijacking that is a common tool for less technically competent attackers. BEC attacks are usually done by compromising a mailbox. The attack begins with a phishing mail to steal credentials and then log in to the victim mailbox from the outside to add forwarding rules. The attacker then monitors the mail traffic and once a promising exchange has been identified.

Data theft of intellectual property is in many ways the silent threat to enterprises. The overall scale of the problem is difficult to gauge, though, as victims may never be aware of a successful attack. The costs of intellectual property theft on an enterprise can also be difficult to measure as the damage mostly affects the victim's long-term profitability, not the short-term earnings. The largest threat to intellectual property today is the massive state-sponsored hacking operations attributed to China.

Attack Vectors

The initial attack vector, or entry point, describes how the attacker obtains access to the first system in the target environment. Understanding how the threat actor obtained access helps in identifying the weaknesses of the organization, the sophistication level and methodology of the threat actor, as well as trends for commonly used attack techniques.

Measuring cyber threats in statistics is fraught with methodological problems, however, such as the difficulty in comparing unlike values such as the number of password-spraying attacks against the number of phishing mail attacks. We have consequently chosen to base the numbers below primarily on successful, or at least partially successful, attacks.

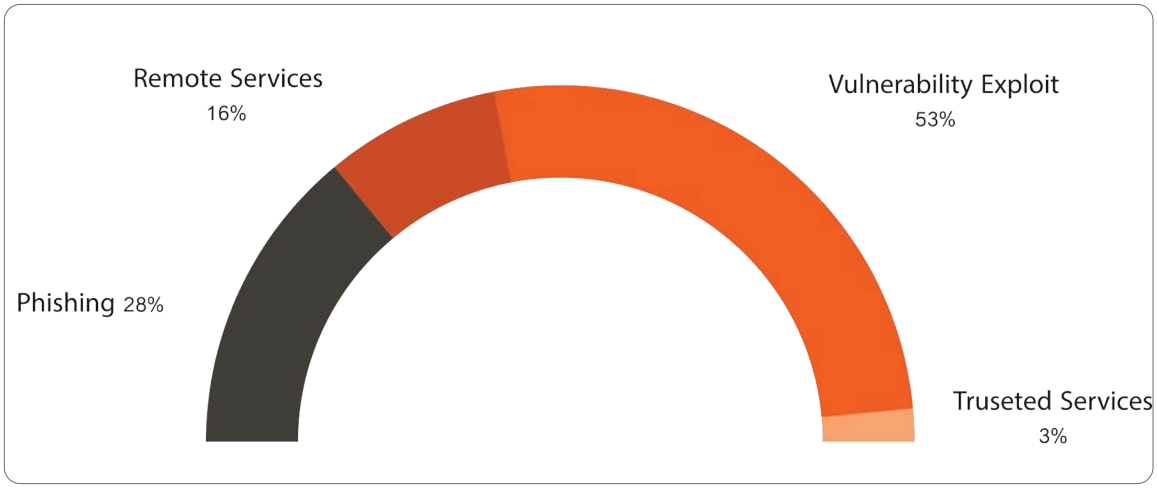

Figure 2: Attack vectors used in cyberattacks against victims in Sweden, January to June 2021 (Source Truesec)

As seen in the chart, phishing emails remain a popular method. Roughly half of all successful cyberattacks in Sweden in 2021 began with a phishing email. Truesec has also observed phishing kits that include MFA relay functionality that allows an attacker to bypass multi-factor authentication.

Truesec has seen a steady rise in other attack vectors, however, especially vulnerability exploits. The COVID-19 pandemic has led many organizations to rapidly build infrastructure that enables remote working. At the same time, attacks targeting vulnerabilities in external-facing services such as VPN solutions have increased substantially. The same is also true for collaboration platforms, which have also been used extensively as part of phishing campaigns, leveraging the fact that many users had to quickly adapt to the remote working conditions due to the COVID-19 pandemic.

While most effective zero-day exploits can be attributed to nation-state threat actors, cybercriminals have become very quick at exploiting such vulnerabilities once they are published. When a critical vulnerability is published, organizations now often have less than 48 hours to patch their systems before an exploit kit that targets the vulnerability is used in the wild by cybercriminals.

Dark Web/Underground Forum Discussion of the Swedish Finance Sector

Customer Availability Drives Theft of Debit and Credit Data

In a dominant percentage of cases, criminals on dark web and underground forums and marketplaces prefer to target financial organizations' customers rather than the organizations themselves, and this holds true for the Swedish market. Availability of victims was very likely the key factor for determining criminal discussion in 2021. A Recorded Future Platform query for references to major Swedish financial institutions on criminal marketplaces in the first half of 2021 showed that the proportion of references across different institutions roughly aligned to number of customers. For example, Swedbank has around 7 million customers and Nordea Bank has approximately 10 million customers, and we found around 3,000 references to Swedbank and about 4,000 references to Nordea. Or, put another way, the ratio of references across Nordea Bank, Swedbank, and SEB Group was 2.5:1:2, and the ratio of customers for these organizations was 2.5:1:1.75, which is remarkably similar.

Alternatively, the number of references to major Swedish banks like Nordea, SEB Bank, Svenska Handelsbanken, and Swedbank compared to those for smaller Swedish banks like Avanza or ICA Banken in the first half of 2021 was at a ratio of roughly 80:1. We found very little criminal discussion of the latter category, with most being Russian Market sales of compromised Avanza Bank logins. There were no other cyber threats to this category of smaller banks aside from 7 credential leaks.

When looking at a general query for the Swedish finance sector compared to queries for major individual banks like Swedbank or SEB Group between January and June 2021, we noted a 5:1 ratio of references to debit versus credit. This is in line with debit and credit card ownership trends in the country; per this report from J.P. Morgan, Swedes prefer debit over credit, and "card penetration remains high in the country at 1.1 debit cards per capita". This data point further supports the hypothesis that availability of targets is a fundamental factor in cyber criminal activity. By contrast, when looking at dark web references for the finance sector internationally, credit card references were notably greater than debit card references.

LockBit 2.0 Ransomware Operators Publish Swedish Data on Extortion Site

While the volume of references to Swedish ransomware victims is much lower than victims of debit or credit card data theft, their prominence in mainstream news has arguably been higher. The most prominent example is likely that of Swedish finance broker Aktieinvest, which in October 2021 became a victim of the LockBit 2.0 ransomware operators, making them the second Swedish victim to appear on LockBit's extortion site after plastic parts manufacturer Prototal Industries.

LockBit 2.0 has consistently appeared in our research as an attacker against European organizations. Between January and October 2021 alone, we identified over 150 instances (some of them rollups of multiple events) in which LockBit operators targeted European victims and posted their data to their extortion site. LockBit Ransomware was first observed in the wild in September 2019, and its operators continue to remain active with the release of LockBit 2.0 in June 2021. In August 2021, LockBit 2.0 operators were observed on social media websites and forums recruiting insiders from large organizations as "affiliates" in an effort to gain initial access to these targets. The operators enticed potential affiliates with million-dollar payouts if information or actions that the affiliate took resulted in a ransom payment by the victim organization.

LockBit 2.0 operators have provided their affiliates with an automatic exfiltration tool dubbed StealBit to run before executing the ransomware payload. The tool automatically gathers and exfiltrates sensitive company data from a victim environment. LockBit 2.0 affiliates may connect to the victim device or devices via RDP by abusing legitimate RDP account credentials, instantiating a C2 channel to be used for exfiltration or to download further programs or payloads.

Aside from sales of customer debit or credit information and a few publications of Swedish companies on extortion sites, we observed few notable references to Swedish financial organizations on dark web or underground forums. In June 2021, a member of Exploit Forum asked if anyone was willing to sell a "nordea Denmark panel" (likely meaning they were looking for compromised access to a control panel for a Nordea server). We saw no responses to this request, although there may have been private replies.

DDoS Attacks Pose High Threat to Finance in 2021

Background: DDoS Attacks Grow Stronger in Past 5 Years

The recent emergence of DDoS as a major threat against financial organizations, including Swedish financial organizations, is simply a new development from a longstanding attack vector. DDoS attacks have increased in frequency and severity in the past several years. According to data from Akamai, from 2015 to 2018 the largest observed DDoS attack increased by over 400%, culminating in a 1.3 Tbps attack on Github in 2018 which lasted for approximately 15 to 20 minutes.

The overall volume of DDoS attacks dipped year over year in 2018, likely a result of coordinated takedowns of DDoS-as-a-service (DaaS) operators by the US Federal Bureau of Investigation (FBI) and Europol. DaaS services provide a low barrier of entry for criminals and hacktivists since they require a little technical sophistication on the part of the purchaser. The respite from DDoS attacks following these takedowns was short-lived, and volumes have continued to increase since 2019. According to a white paper published by Cisco and last updated on March 9, 2020, "Globally, there was a 776% growth in attacks between 100 Gbps and 400 Gbps Y/Y from 2018 to 2019, and the total number of DDoS attacks will double from 7.9 million in 2018 to 15.4 million by 2023".

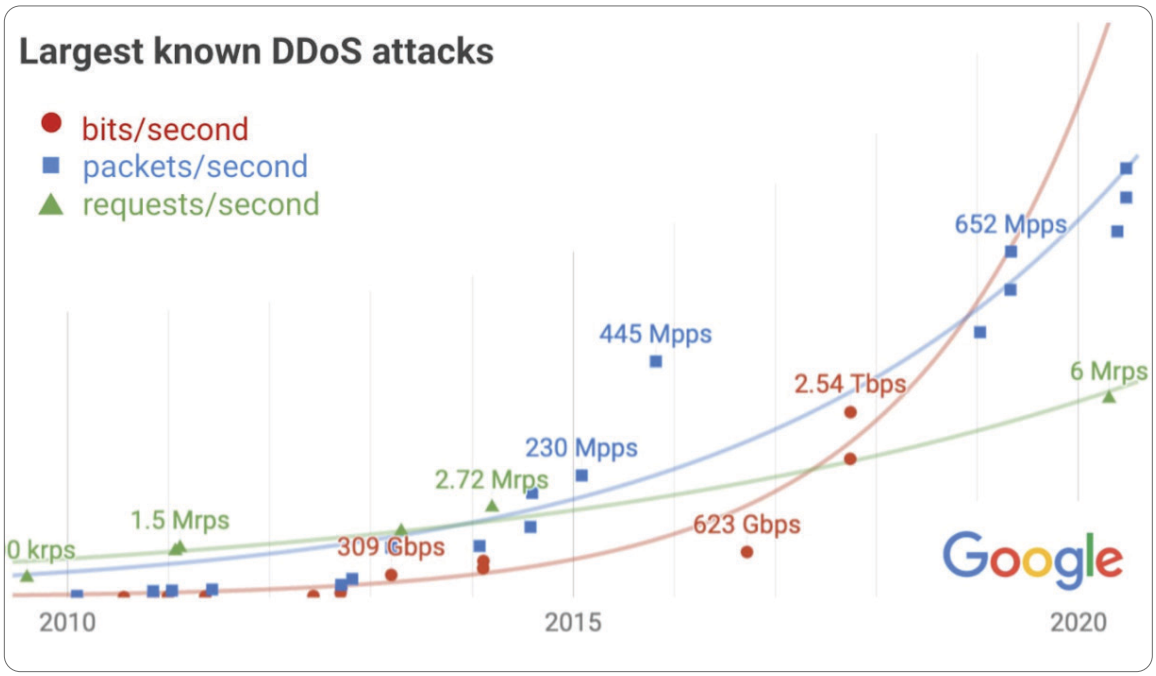

Figure 3: Largest-known DDoS attacks between 2010 and 2020, showing a roughly 600-fold increase (Source: Google Cloud)

According to a press release on June 14, 2021, researchers from Nokia Deepfield announced that they had conducted a study of global network traffic from January 2020 to May 2021, including traffic from thousands of routers across multiple ISPs, and found that "the origins of most of the high-bandwidth, high-intensity (volumetric) attacks [come from] a limited number of internet domains … most global DDoS attacks (by frequency and traffic volume) originate in less than 50 hosting companies and regional providers". The study also found a 40-50% rise in DDoS traffic since the implementation of COVID-related lockdowns globally. A large amount of this traffic was attributed to the accessibility of DaaS.

Along with hacktivists and cybercriminals, state-sponsored attackers also employ DDoS attacks. On October 16, 2020, Google reported that it had mitigated a UDP reflection attack peaking at 2.54 Tbps. Google's Threat Analysis Group (TAG) traced the attack to Chinese ASNs and implicated that it was state-sponsored, with a majority of the traffic originating from 4 Chinese internet service providers (ISPs) ASNs: 4134, 4837, 58453, and 9394. State-sponsored actors have also targeted the US financial sector directly using DDoS attacks. In 2016, 7 Iranians were charged in connection to Operation Ababil, a multi-phase series of DDoS attacks targeting multiple US financial institutions including Bank of America, PNC, CapitalOne, Zions bank, and JPMorgan Chase & Co.

Between January and October 2021, Recorded Future logged nearly 85,000 references to DDoS attacks from dark web and underground forum sources, showing the high amount of criminal attention to this attack type. In some cases, these references involved criminals' desire to protect their infrastructure against DDoS attacks, but in the vast majority of cases, these references involved criminal sales of DDoS attack services to a number of different types of clientele.

Several cybercriminal groups aim to place trojans on computers that transform them to large "botnets" to spread spam, other malware or for DDoS attacks. To rent a botnet for DDoS attacks can cost anything from $20 to $300 for a sustained DDoS attack from a thousand bots over a few weeks. It is more expensive to rent botnets with infected computers from Europe and the USA as computers there typically have better bandwidth. Bots from Asia and Africa are also easier to filter by DDoS protection.

The market for DDoS attack services has existed for at least a decade. Within the past 5 years, the typical cost for this type of service has been $50-$200 USD per day (such as advertised in 2016, 2018, and 2021) depending on whether the purchaser wants a "weak" or "strong" attack. As one might anticipate, DDoS attacks against strongly defended sites command a premium cost; for example, in 2016, attacks against strong defenses were advertised at between $200 and $500 per day. The emergence of DDoS mitigation services like Cloudflare has also created new opportunities for criminals, who have offered more expensive DDoS attacks specifically to bypass these types of protections (such as advertised in 2016 up to 2020). DDoS providers also occasionally mention what layer of the OSI model (Layer 4 or 7) their attacks are effective against, such as a botnet that "specializes in Layer 7 attacks" (per this 2017 advertisement).

A typical DDoS attack can consist of anything from 1,000 up to 20,000 or more bots. For cybercriminals, this represents the investment that they make in their criminal venture. Consequently, even a relatively small ransom demand, as low as $100,000, can represent a very profitable return.

DDoS attacks can also be parts of a larger cybercrime attack. Ransomware syndicates such as REvil now threaten to conduct DDoS attacks against victims of ransomware to apply further pressure to victims and induce them to pay the ransom. Sometimes DDoS attacks can also be used to distract the target's incident response capacity and mask other intrusions, although this is less common.

It is difficult to identify the threat actors behind DDoS attacks. While a small number of attacks are conducted by lone hackers who are motivated by hatred or conspiracy theories, the majority of attackers are cybercriminals looking to extort their victims for money. Through analysis of the IP addresses involved in an attack, it is sometimes possible to identify which botnet is used as a platform for the attack, but it is seldom possible to determine who rented the botnet to perform the actual attack. The number of DDoS attacks is estimated to have increased by 50% in 2020 compared to 2019. So far, this upward trend has continued in 2021.

Several factors drive the increase in DDoS attacks:

- The COVID-19 pandemic has led to an increase in the use of VPNs and other collaboration platforms, which in turn has led to more vulnerable attack surfaces.
- There are now trojans that target internet-of-things (IOT) devices
- The bandwidth on the internet continues to increase.
- Cybercriminals have discovered that many victims will reliably pay the ransom money.

The problem of trojans infecting IOT devices in particular is expected to grow, as these devices are often unprotected. The rollout of fifth-generation cellular networks (5G) and their even greater bandwidth will further exacerbate these problems.

DDoS Attacks Find Success Against Swedish Financial Targets

While DDoS ransom is only a small portion of all cybercrime attacks, it represents all known successful attacks against financial institutions in Sweden. Financial institutions have been exposed to cybercriminals for a longer time than many other business sectors, so their networks are overall better protected against breaches. Ransomware gangs are often opportunistic and prefer easier targets. At the same time, financial institutions can be uniquely vulnerable to denial-of-service attacks, as they rely so much on fast and reliable transactions over the internet.

In 2021, a Swedish financial institution was the target of a DDoS attack. The attack lasted for roughly 3 weeks and consisted of sustained attacks, each lasting from 10 to 30 minutes against multiple IP addresses. Overall, this attack mapped well to many of the attack patterns available to rent from various botnet operators.

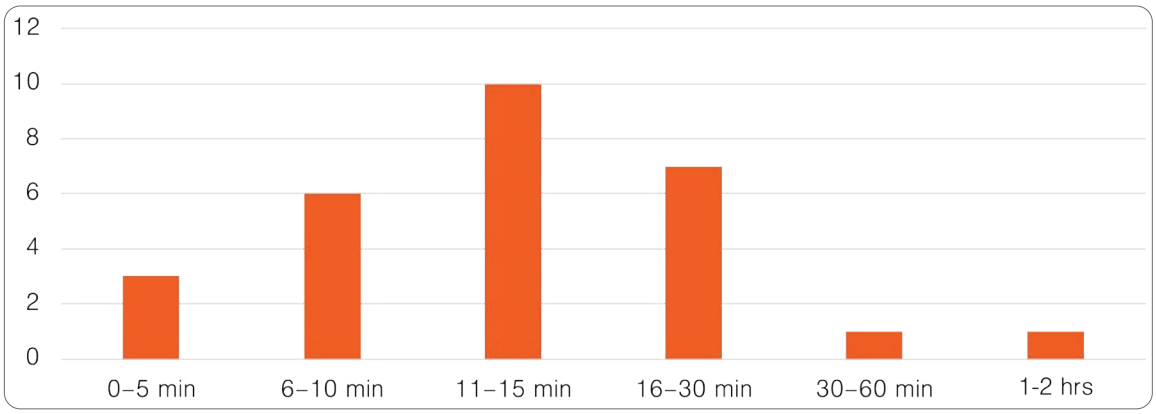

Figure 4: Average lengths of DDoS attacks against victims in Sweden in 2021. The outliers over 30 minutes may represent 2 consecutive attacks. (Source: Truesec)

Analysis of the attack patterns shows that the attack did not seem very sophisticated. The main targets were 2 IP addresses associated with easily identifiable domains that are used for customers to log in. A more sophisticated attacker could have taken time to map the network with tools like Shodan to identify other vulnerable IPs where temporarily disrupting connections would cause greater damage.

Even though the victim had a relatively expensive DDoS protection service and the attack wasn't very sophisticated, it still degraded and disrupted service on the targeted IP addresses. To understand why it is important to understand more about different types of DDoS attacks.

There are two main forms of DDoS attacks: volumetric attacks and application-based attacks.

- A volumetric attack consists of a mass of Layer 3 (ICMP) or Layer 4 (UDP) connections, such as simple SYN packets that overwhelm the connection. This is also known as SYN flooding. The severity of the attack is determined by the combined bandwidth of the attackers.
- An application-based attack consists of Layer 7 connections, usually HTTP or HTTPS. The most common form of attack is to send a HTTP request that simulates a request larger than one packet. The victim machine recognizes that it must wait for the second packet, holding the connection occupied, but no second packet is sent.

A typical DDoS attack, such as the attack described above, consists of a combination of both volumetric and application-based attacks. Below is the distribution of different types of attacks that Truesec investigated. The preponderance of Layer 7 attacks may represent the attacker adapting to use these attacks where most successful.

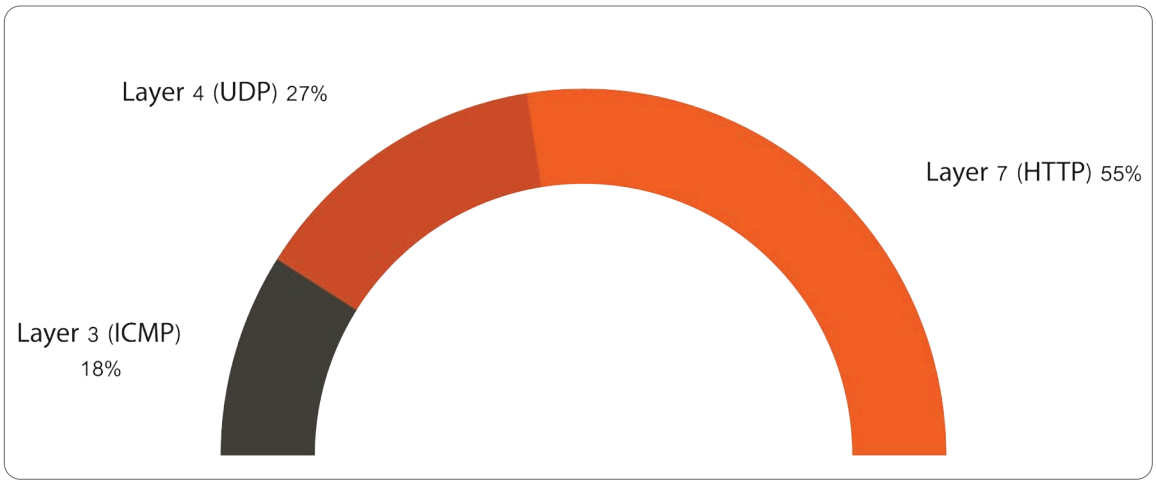

Figure 5: Distribution of DDoS attack types used in cyberattacks against victims in Sweden in 2021. The attack types here target Layer 3 (via ICMP), Layer 4 (via UDP), and Layer 7 (via HTTP). (Source: Truesec)

A good DDoS protection service can, in principle, halt both types of attacks. However, stopping application-based attacks is harder than stopping volumetric attacks. Filtering out application-based attacks requires tuning the DDoS protection product to recognize HTTP traffic that normally occurs on the IP, but filtering malicious traffic this way is complex. Providers of DDoS protection products and services can do the tuning for the customer, but this is typically a costly service. This is also a cost that is often not fully revealed to the customer until after the purchase, at which point some customers balk at the additional cost. The result is that many organizations that have bought full DDoS protection have products that are badly tuned to protect from Layer 7 attacks without realizing until it is too late.

Outlook and Recommendations

The lack of news about major cyberattacks against Swedish organizations relative to news about other countries reflects a strong symbiosis between the country's overall implementation of information security and its culture of reporting cyberattacks quickly and transparently. However, fewer mainstream reports of attacks does not mean that Swedish institutions, especially in the finance industry, have been immune from cyberattacks in 2021; based on the data identified by Recorded Future and Truesec, Swedish financial organizations have a few major threats to watch for into 2022, including DDoS and ransomware attacks.

The following mitigations can be implemented to protect against and reduce the negative effects of DDoS attacks:

- Enroll in a DDoS mitigation service that detects and profiles abnormal traffic flows and redirects traffic away from your network, including those where Layer 7 protection is involved. It is essential that any service under consideration demonstrates that protections are in place across many different types of application protocols.
- Use services provided by Content Delivery Networks (CDNs) or providers specializing in DDoS mitigations to filter traffic upstream from services.
- Test and document your DDoS detection and recovery capabilities before an incident.
- Consider throttling UDP packets with lengths greater than 468 bytes that are sourced from known amplification ports, such as: 1-1023, 1194, 1434, 1900, 3074, 3283, 3702, 5683, 11211, 17185, 20800, 27015, 30718, 33848, 37810, 47808.
    - Rate-limiting these ports may cause a loss of functionality on production networks. Test these changes on a non-production network and advise all customers before deploying this mitigation.
    - Closely monitor recursive DNS servers, which may need to receive large responses from port 53.
- Review alerting capabilities via netflow monitoring.
- Institute BGP null routing. If you have the ability to BGP null route traffic prior to an attack, you can thwart all activity from an attacker's IP address.
    - Set up rate limiting. Where possible, rate-limit both connections and bandwidth within legitimate baselines, from routers all the way to applications. Apache ModSecurity is an example of a tool that can help in this regard.
- Use a service for filtering by traffic type. Being able to filter malicious distributed traffic from legitimate connections is key to combating a DDoS attack without affecting normal operations. Several companies provide this service, including Arbor, Cloudflare, and Akamai.
- Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.
- To defend against SYN floods, enable SYN cookies.
- Configure network firewalls to block unauthorized IP addresses and disable port forwarding.
- Ensure all IoT devices are up to date, security patches are incorporated when available, and default passwords are changed on all devices.

The following mitigations can be implemented to protect against and reduce the negative effects of ransomware attacks:

- Ransomware often follows a specific pattern of behavior that can be detected with a robust threat intelligence system, integrated with SIEM platforms.
- Implement YARA rules like the ones found in Recorded Future hunting packages to identify malware via signature-based detection or SNORT rules for network-based detections. Ransomware specific hunting packages can be found with this query.
- Use Recorded Future identification of malicious servers to block or alert on observed traffic in your environment.
- IOCs can be used to proactively query or scan BMGI environments for items such as file hashes, registry keys, and IP traffic associated with ransomware.
- Maintain updated, offline backups of sensitive data to prevent data loss in the event of a ransomware infection.
- Network segmentation can halt the propagation of ransomware through an organization's network. This solution involves splitting the larger network into smaller network segments and can be accomplished through firewalls, virtual local area networks, and other separation techniques.
- If remote access solutions are crucial to daily operations, all remote access services and protocols, such as Citrix and RDP, should be implemented with multi-factor authentication. Exposed Remote Desktop Protocol (RDP) servers are also abused by threat actors to gain initial access into a target's network. Threat actors will look for networks that have internet-facing servers running RDP and then exploit vulnerabilities in those servers or use brute-force password attacks. Once inside the network, the threat actors move laterally and install ransomware on target machines, often disabling backups and other protections.
- Through the use of process monitoring, monitor for the execution and command of binaries involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit.
- Monitor for the creation of suspicious file modification activity, particularly large quantities of file modifications in user directories.
- Consider keeping sensitive client information on systems that are disconnected from the internet or segmented from the rest of the corporate network. Since ransomware will encrypt all files on a victim system and often will search for directories on the network (like networked file shares) to also encrypt, moving highly sensitive customer data to systems with no internet access and minimized access to the rest of the network will limit the access ransomware would have to those files.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.

About Truesec

Truesec is a global cybersecurity company with a clear purpose: Creating safety and sustainability in a digital world by preventing cyber breach and minimizing impact. Over the years, Truesec has gained a strong reputation and earned the trust of organizations worldwide. Today, Truesec consists of 200 dedicated cyber specialists covering the full spectrum of cybersecurity.

Learn more at truesec.com and follow us on Twitter at @Truesec.