Threat Intelligence Report 2024

An In-Depth Analysis of
the Cyber Threat Landscape

TRUESEC

Sheraton

Contents

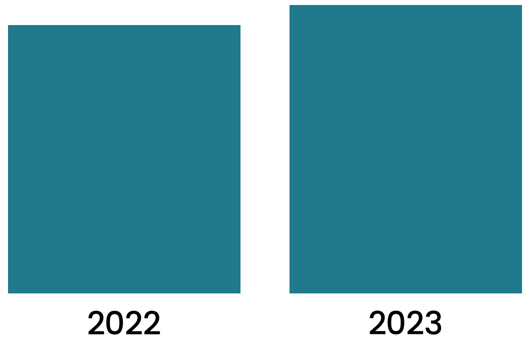
Overview of the Cyber Threat Landscape

Facts and Figures

In this first section of the report, we'll provide an overview of current threats based on data and statistics from Truesec's extensive experience in preventing breaches and minimizing impact.

The rise in the number of ransomware attacks in the Nordics in the last few years appears to have reached a plateau in 2023.

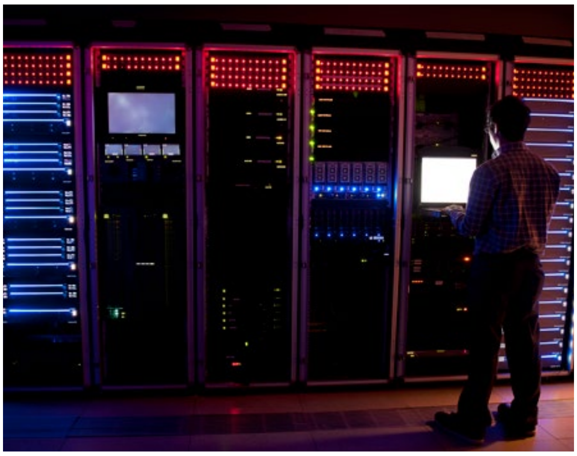
Ransomware Attacks per Year



Many factors may have contributed to this development; however, the largest enterprises have likely begun to improve their cybersecurity, so they're no longer easy targets. Overall, ransomware appears less targeted and more opportunistic than last year – ransomware criminals strike where they can get in. Ransomware groups will move down to smaller victims with a better chance of success, even if those victims can't afford large ransom amounts.

The most prolific ransomware group in the Nordics in 2023, Akira Ransomware, has used a mixture of stolen credentials and exploiting vulnerabilities. Akira operators appear to primarily target smaller organizations with less than 500 employees.

One reason could be that larger organizations have become better at enforcing MFA, which makes using stolen credentials as an initial attack vector more difficult. Another reason could be an influx of new cybercriminals that can only conduct simple ransomware attacks against smaller targets.



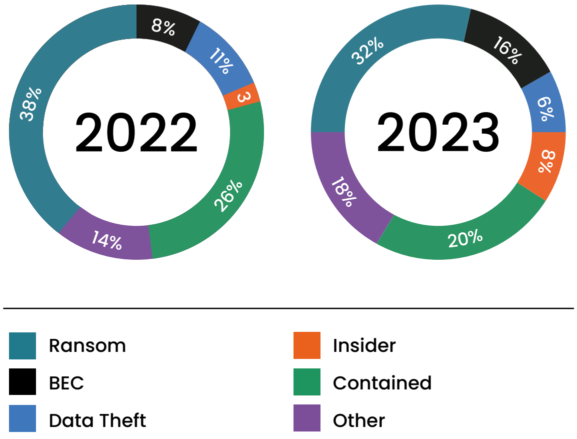
Looking back at our 2023 report, it's clear that we haven't observed the anticipated rate of increase in ransomware. While there are many new actors, they're still not nearly as efficient as the older, more experienced ransomware groups. There's also some gatekeeping among ransomware criminals, as the top ransomware-as-a-service groups charge a flat fee of thousands of dollars just to join.

It's important to understand how much ransomware has become a business today. Each attack represents an investment in time and money to buy tools. As this business matures, different actors specialize in different ecosystem niches. A novice might be limited to free tools, such as password-spraying scripts and publicly available exploits to old known vulnerabilities. Established ransomware syndicates on the other end of the spectrum can invest hundreds of thousands of dollars to access valuable networks.

It's also evident that while the number of successful ransomware attacks has not increased, the number of attacks continues to rise. Looking at statistics from our SOC, the number of intrusion attempts has doubled since the war in Ukraine began in February 2022. Some of this may be due to increased automation of intrusion attempts. It's clear that the number of serious cyber incidents has ceased to rise, not because the threat itself has ceased to grow but because more organizations have upgraded their defenses.

Different Types of Attacks

There's no obvious discernible trend in the different forms of serious cyber incidents Truesec handled in 2023 compared to the previous year. The same types of cybercrime as last year still dominate the scene.



Ransom attacks consist mainly of ransomware attacks, but other forms of cyber extortion also fall under this category. Though not common, some cybercriminals only steal sensitive corporate data and use it as ransom without encrypting the environment. Another type of ransom attack that has continued in 2023 is distributed denial of service (DDoS) extortion. Threat actors direct DDoS attacks against corporations with a significant internet presence and demand ransom in cryptocurrency to stop the attacks.

Business email compromise (BEC) is a cyber attack that relies exclusively on weaponizing access to corporate mailboxes to steal money. The attack usually begins with phishing mail to steal credentials, followed by a login to the victim's mailbox to add forwarding rules. The attacker then monitors the mail traffic, and once a promising exchange has been identified, the attacker hijacks the conversation and modifies the banking details to redirect the payments.

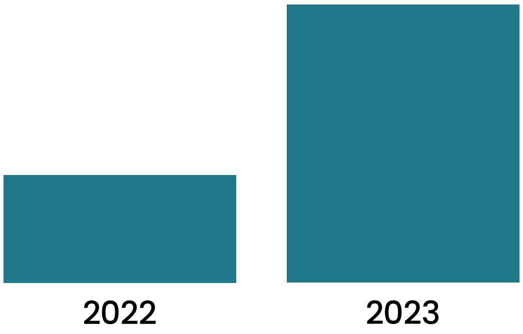
Contained attacks are when a threat actor obtains access to a network with the intent to use the access either for criminal purposes or to sell the access to other criminals but is stopped in time. That so many cyber attacks are stopped after the breach but before a threat actor can use the access to cause real harm shows the importance of having proper detection and mitigation capabilities. In these cases, the final objective is not always certain.

Insider incidents are when a malicious insider has either stolen data or purposely damaged parts of the network. We've observed an increase in this type of incident in 2023; this may be connected to layoffs in the IT industry resulting from the economic downturn.

As we previously noted, the actual numbers of ransomware attacks have remained relatively static in 2023 compared to 2022. The relative decrease in percentage has occurred against the backdrop of an increase in the overall number of cyber attacks.

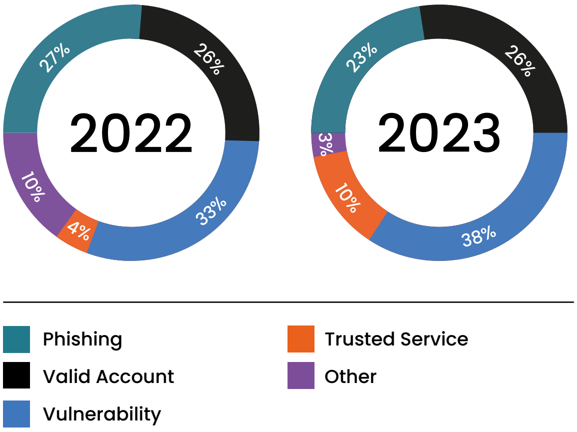
Most notable is the increase in BEC attacks. In real terms, the number of BEC attacks observed has increased by 160% compared to 2023. It's believed that this increase is partly due to new, more sophisticated threat actors being involved in this type of cyber attack.

BEC Attacks per Year



Attack Vectors

Looking at the initial attack vectors used in serious ransomware cases, we can observe that the three most common attack vectors remain the same: phishing emails, vulnerability exploits, and stolen or brute-forced credentials to remote services, such as VPN and RDP.

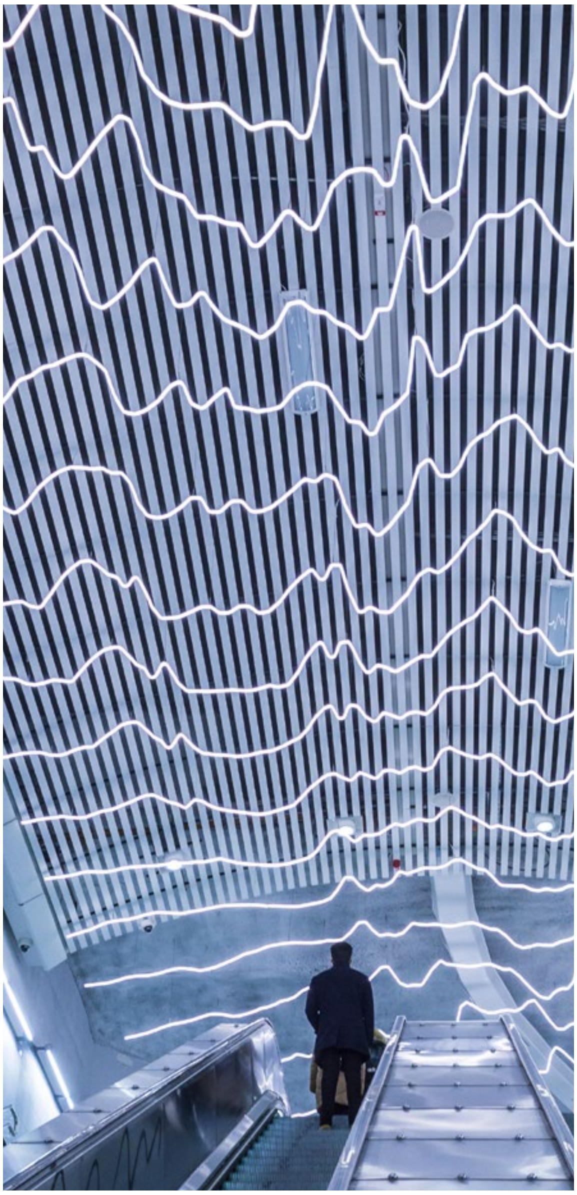


These attack vectors are not mutually exclusive either. Many access brokers use phishing emails that direct the victim to a fake login page designed to steal the victim's credentials. Ransomware actors buy these credentials and use them to breach networks, sometimes months later.

In 2022, we observed a rise in exploitation vulnerabilities as initial attack vectors, and in 2023, this trend has been magnified. Almost 40% of all cyber attacks handled by our Incident Response Team involved the exploitation of a vulnerability in an internet-facing service to gain entry. There are two likely reasons for this: Many serious vulnerabilities have been published this year, and increased use of MFA in organizations has made selling stolen credentials less effective.

When ransomware criminals use mass exploitation of vulnerabilities in external-facing systems to breach networks, it's common that they first establish additional persistence in the form of web shells or other backdoors. Then, they can return to the victim later to conduct the actual ransomware. The advantage of this method for the attacker is that they have installed persistence that will remain even if the victim patches their systems after seeing that a vulnerability can be exploited for ransomware.

Another significant trend is that supply chain attacks, which involve compromising trusted services from third-party vendors, are a growing threat. While still only used by the top ransomware groups, this appears to be an increasing problem.



Ransomware Victims

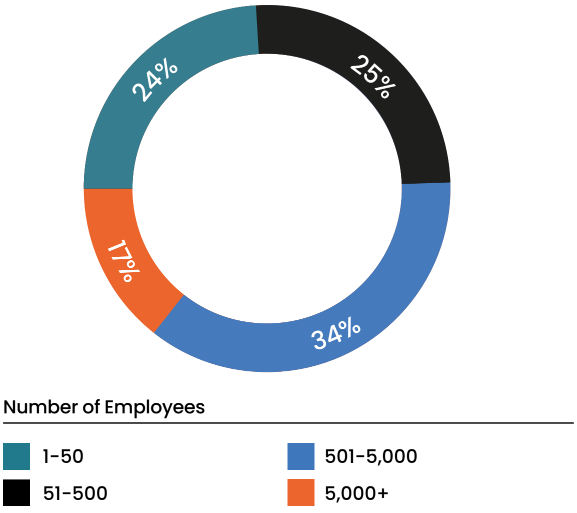
Big ransomware syndicates often prefer to target larger corporations that can afford higher ransom amounts, but in 2023, Truesec observed that ransomware groups were increasingly hitting smaller enterprises.

A likely reason is that many large enterprises are now aware of the need for cybersecurity and also have the resources to invest in proper cybersecurity. They've improved their defenses and acquired effective managed detection and response capabilities. This makes them more difficult targets to breach, so cybercriminals move on to easier victims.

Some large enterprises still have vulnerabilities that expose them to ransomware, usually in the form of legacy systems deemed too expensive to replace. This still makes them "low-hanging fruit" for the ransomware criminals. However, just because cybercriminals are now targeting smaller organizations doesn't mean that large enterprises can relax.

Cyber attacks are constantly evolving, and the work of maintaining comprehensive cybersecurity never ends. The numbers indicate, however, that if organizations take cybersecurity seriously, then the risk of crippling ransomware attacks and other cyber attacks can be reduced significantly.

Distribution of Ransomware Attacks Against Different Sizes of Organizations



This also means that medium-sized enterprises will have to learn the same painful lessons that many of the largest corporations have already learned: Not investing in cybersecurity can become a costly mistake.

Threat Actors: Ransomware

It's Only Business

The modern ransomware syndicates are now organized businesses. There's an apparent disconnect between how Russian ransomware groups perceive themselves and how their activities are perceived in the West. Many ransomware groups now deliver ransom notes, claiming they're only penetration testers requiring a fee for their services. This may partly be to make the payment more palatable to the victims but could also be something these criminal businesses have internalized as a "truth."

Organized crime, protection fees, and similar extortion are so much a part of Russian business culture that it may have been normalized in the eyes of the criminals. If you have poor cybersecurity, you'll pay the price. That's the rule from their perspective.

Ransomware operators are not hackers searching for thrills or fame. They're motivated purely by financial gain. Understanding these criminals' business models can help you guide your cyber defenses, as not all ransomware groups target the same victims. Some cybercriminals use simple, inexpensive methods. As in many other forms of business, it takes money to make money.

Novice cybercriminals don't have the resources to buy expensive tools or access. They buy inexpensive, primitive ransomware and use simple methods like password spraying or publicly available exploits to vulnerabilities that have been known for a long time. They mainly target smaller enterprises that can't afford professional incident response teams, as cheap ransomware often has flaws that can be used to break encryption without keys, something a good IR team understands.

An advanced professional freelancing ransomware criminal must invest resources into their attacks. They'll sign up to one or more big ransomware-as-a-service groups, sharing their profit. They typically will also have to invest financially in each heist by buying access from an access broker. At this stage, the ransomware criminals are also invested in understanding their victims.

The typical access broker will be opportunistic in their approach to access gathering, often using a combination of phishing and brute-force password spraying to gain access to vulnerable networks. They then conduct quick online checks for the annual turnover of the company they have access to and try to sell the credentials to ransomware criminals. This will, on average, cost between 1,000 and 10,000 euros per access, depending on the company's size. This cost represents a freelancing ransomware criminal's investment for every attack.

The top-tier ransomware groups operate large teams of cybercriminals working together to breach networks and deploy ransomware. These cybercrime syndicates represent the most advanced and diverse threat to organizations. They continually invest in developing custom tools, infrastructure, and salaries for their employees. They prefer to select relatively large companies as targets for their attacks, as they want a return on their investment in the form of a multimillion-dollar ransom to make the attack worth their investment in time and money, something only more prominent victims can afford.

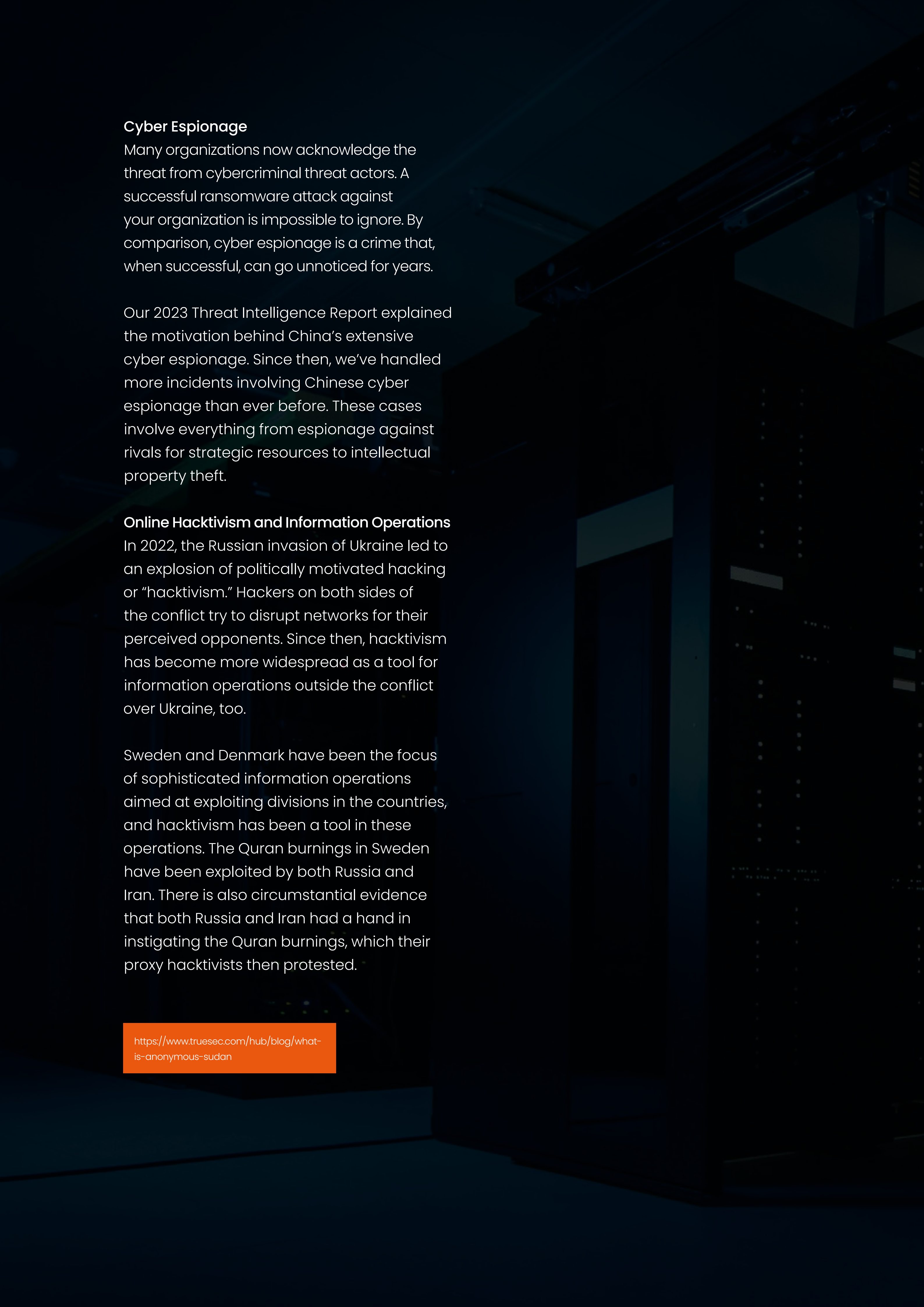
More Ransomware Groups Than Ever

In our 2023 Threat Intelligence Report, we forecasted that we would see a further rise in ransomware due to Russia's continuing isolation and economic deterioration. As opportunities to pursue a typical career in IT that can support a decent life decrease in Russia, the lure of organized cybercrime will likely appear acceptable to more and more individuals in the Russian IT sector.

Since then, we've observed more new ransomware groups than ever before, so keeping track of all the groups and their affiliations has become nearly impossible. Out of all the ransomware cases we handled in 2023, over 50% involved groups we had never heard of before that year. There's a constant flux and rebranding of ransomware actors as the criminals try to make it harder for security researchers to track them. However, the sheer number of actors in 2023 suggests that some of these actors are new to the ransomware ecosystem.

The influx of new cybercriminals appears to have created some internal tensions among the cybercriminals when old criminals accuse new players of not following unwritten rules. This appears to have led to open conflict between older and newer affiliates in the LockBit ransomware-as-a-service syndicate when veterans accused newer affiliates of settling for too low ransom payments, which they claim complicates their own negotiations.

As the new ransomware actors get absorbed into the established ransomware ecosystem, their skills likely mature, and their respect for the internal rules is established. The extent of this consolidation may ultimately depend on the overall stability of the Russian state, but taking these factors together, the likely outcome is that we will see more and better-trained ransomware criminals in the future, leading to more attacks.



Cyber Espionage
Many organizations now acknowledge the threat from cybercriminal threat actors. A successful ransomware attack against your organization is impossible to ignore. By comparison, cyber espionage is a crime that, when successful, can go unnoticed for years.

Our 2023 Threat Intelligence Report explained the motivation behind China's extensive cyber espionage. Since then, we've handled more incidents involving Chinese cyber espionage than ever before. These cases involve everything from espionage against rivals for strategic resources to intellectual property theft.

Online Hacktivism and Information Operations
In 2022, the Russian invasion of Ukraine led to an explosion of politically motivated hacking or "hacktivism." Hackers on both sides of the conflict try to disrupt networks for their perceived opponents. Since then, hacktivism has become more widespread as a tool for information operations outside the conflict over Ukraine, too.

Sweden and Denmark have been the focus of sophisticated information operations aimed at exploiting divisions in the countries, and hacktivism has been a tool in these operations. The Quran burnings in Sweden have been exploited by both Russia and Iran. There is also circumstantial evidence that both Russia and Iran had a hand in instigating the Quran burnings, which their proxy hacktivists then protested.

https://www.truesec.com/hub/blog/what-is-anonymous-sudan

The DDoS Ecosystem Explained

As explained previously, hacktivism mainly relies on DDoS attacks. Smaller DDoS attacks can be generated by tools available to download for hacktivists, but larger DDoS attacks rely on a criminal ecosystem of DDoS providers. The major hacktivist groups don't control their own resources in the form of botnets, rented servers, or hacked clients to use as a base for DDoS attacks. Instead, they rent capacity from providers. Russian hacktivists have even begun to advertise what DDoS service they use, likely to get a reduced price for helping to promote the service.

Overall, it's unclear if the number of DDoS attacks has continued to increase compared to 2022; however, the intensity of the attacks appears to have increased. Major DDoS providers now have more power to conduct stronger attacks, and state-sponsored hacktivists are willing to pay for it.

This means virtually no hacking skill is involved in heavy DDoS attacks. Sometimes, all that's required is a credit card. This is why almost anyone can become a DDoS hacktivist. The only limit is the cost of the attack.

At the top are notorious groups, like Anonymous Sudan, with many followers and support from a government that can afford the most disruptive DDoS attacks. Many hacktivist groups also actively solicit funds from their followers on social media. At the bottom are hobby hacktivists, sometimes lone individuals, who use primitive tools to conduct far less impactful DDoS attacks.

Links to Other Threats

The relative ease with which DDoS attacks can be conducted and the notoriety some Russian hacktivist groups have gained today means that other nations are following suit. This summer, an Iranian hacktivist group, Anzu Team, copied the Russian information operation that included attacks by Anonymous Sudan.

There is also a gray zone between primarily Russian hacktivism, disinformation, and cybercrime. Russian hacktivists KillNet have conducted DDoS attacks for the benefit of a known darknet site that sells drugs against a rival site. KillNet has also partnered with a Telegram channel used to monetize disinformation, promoting pro-Russian narratives mixed with crypto scams aimed at Western conspiracy theory believers.

Hacktivism can be seen as a form of crowd-funded cyber vandalism, but it can also be viewed as part of a broader threat from the post-truth disinformation ecosystem.

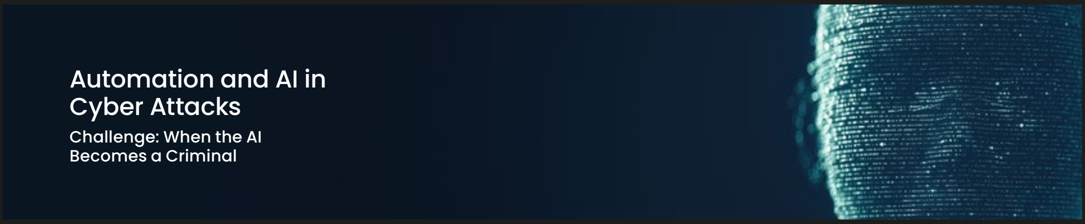
Four Challenges and How To Tackle Them

The second section of the report is a deep dive into specific challenges facing cybersecurity in 2024. By matching Truesec's capabilities in threat intelligence with our many years of experience investigating and preventing cyber attacks in Northern Europe and the rest of the world, we'll help you understand what's happening and what it means for your security.

This year, we must begin by stating that all the challenges we presented in the 2023 Threat Intelligence Report are still valid concerns, as they illustrate techniques still used by cybercriminals. Rather than restate the same challenges, we'll focus on four emerging challenges. This report is intended to be an update to last year's report, not a replacement.

Each chapter details a particular challenge and provides advice on solutions. In addition, we have exemplified many of the challenges with a real-world incident story that illustrates the challenge we explain.

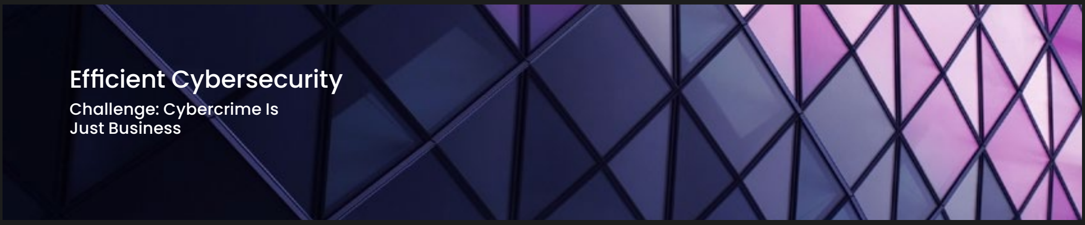
1\.



Automation and AI in Cyber Attacks

Challenge: When the AI Becomes a Criminal

2\.



Efficient Cybersecurity

Challenge: Cybercrime Is Just Business

3\.

New Laws and Regulations

Challenge: Knowing All New Legal Responsibilities

4\.

Protecting Your Digital Assets

Challenge: When the Threat Actor Is Already Inside

Automation and AI in Cyber Attacks

Challenge: When the AI Becomes a Criminal

In recent years, Truesec has observed increased automation in cyber attacks. Malware developers are increasingly providing criminals with complete attack frameworks with easy-to-understand GUIs that make cyber attacks easier to conduct for novices.

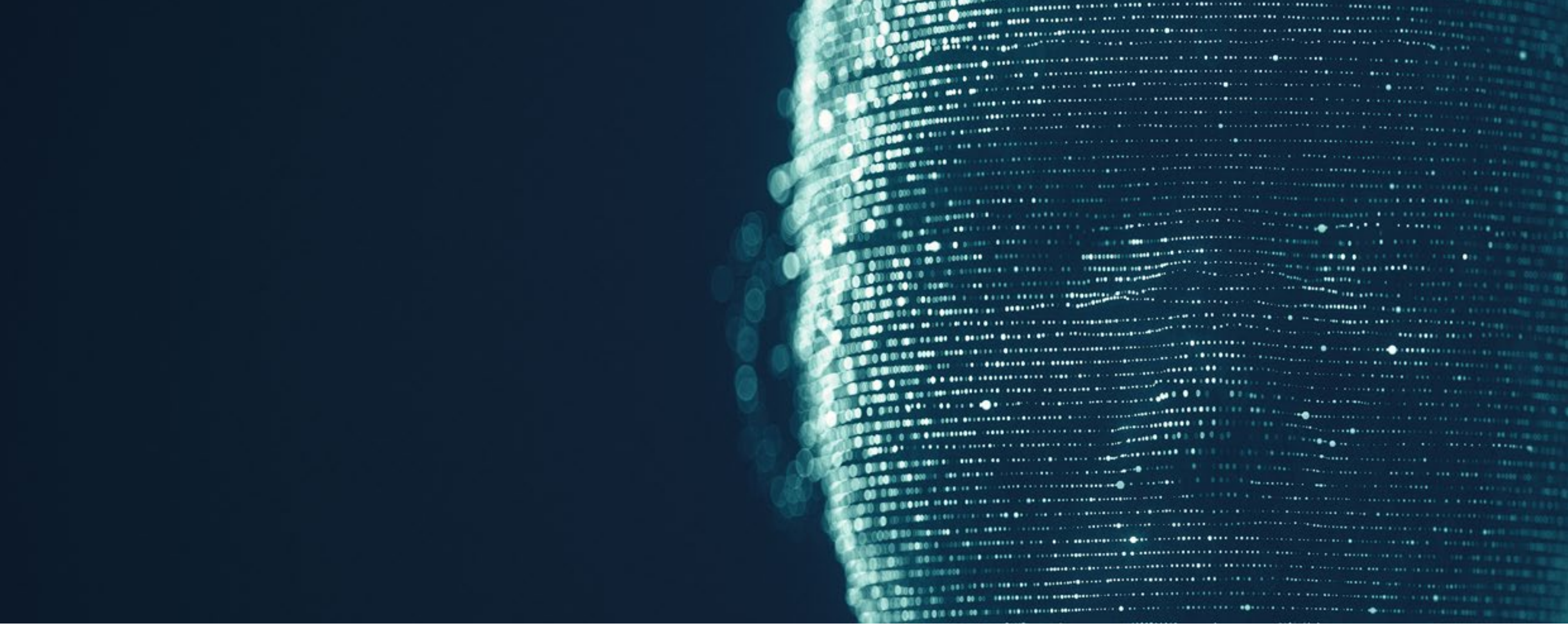
The hope that responsible guards in AI-powered chatbots would limit their use for cybercrime appears to have been dashed. AI researchers have now begun to release AI-powered chatbots that are trained on the dark web and developed specifically to help cybercriminals. The aim is to create malicious AI bots capable of creating sophisticated phishing campaigns, executing social engineering campaigns, exploiting vulnerabilities, and creating and distributing malware.

So far, a few malicious chatbots are now available for use by cybercriminals, including one trained to assist in solving scripting and coding problems and one that can assist cybercriminals in crafting better phishing mail and social engineering attacks.

Cybercriminals will use these tools to improve their attacks and become more efficient in breaching networks. It's still too early to say how quickly this trend will develop or how much it will affect the cybercrime scene, but the likely outcome will be an increase in the threat of cybercrime in the coming year as more and more cybercriminals learn to adopt these tools.

At the same time, it's important not to overstate the effect of cybercriminals using AI in their attacks. The likeliest outcome if cybercriminals begin to adopt AI to assist in their attacks is not that cybercriminals' attacks will be technically more proficient or advanced but that experienced hackers, in some cases, will be faster and more effective in conducting their current attacks. AI chatbots will not replace criminals any more than they will replace developers.

AI chatbots can assist in social engineering attacks, but using such tools to translate text is usually not more revolutionary than using them to assist in coding. They can help someone proficient in a language to translate faster, but if used just as an advanced Google Translate, it will still mostly yield unimpressive results.



Deepfake technology is one area where AI can become real trouble for cybersecurity. With deepfakes and AI-generated images, video, and audio, deception and trust issues arise for companies and personnel. This will inadvertently lead to more attacks that will stress an already overtaxed security department.

If the AI model lacks enough information, the answers delivered can often be biased, which, within security, can lead to mistakes and security risks. Many AI models available are open projects that can be hacked, manipulated, and fed false data. Security teams need to consider how AI and machine learning (ML) models are trained with relevant data to not only provide correct information but also not disclose sensitive or regulated data.

Another risk is that references to research or downloadable content will be filled with low-quality AI-generated content. AI hallucinations in research papers can damage brand reputation. Even AI-generated code libraries can become a problem. AI detection systems are themselves based on AI and ML and thus far from infallible.

Ultimately, AI is just a tool. The greatest cybersecurity risk with AI may not be that it is used as a tool by criminals but that there is now a rush to include AI in processes in many industries. A rush that could lead to the construction of systems that are not properly secured and vetted, creating a technical debt ready to be exploited by future threat actors.

The combination of increased automation, easy-to-use attack frameworks, and trained AI that assists threat actors will not necessarily make threat actors more advanced but more efficient. This means that the cybersecurity requirements will not necessarily change dramatically, but AI and increased automation will increase the danger of ignoring requirements and be "low-hanging fruit" for even faster cybercriminals in the future.

Solution:

Knowledge Is Power

Rightly used, AI can also help bolster our defenses, and cybersecurity companies like Truesec are also investing in AI research to offer even better protection in the future. Today, AI is far from capable of effectively being used alone for cyber attacks or defense.

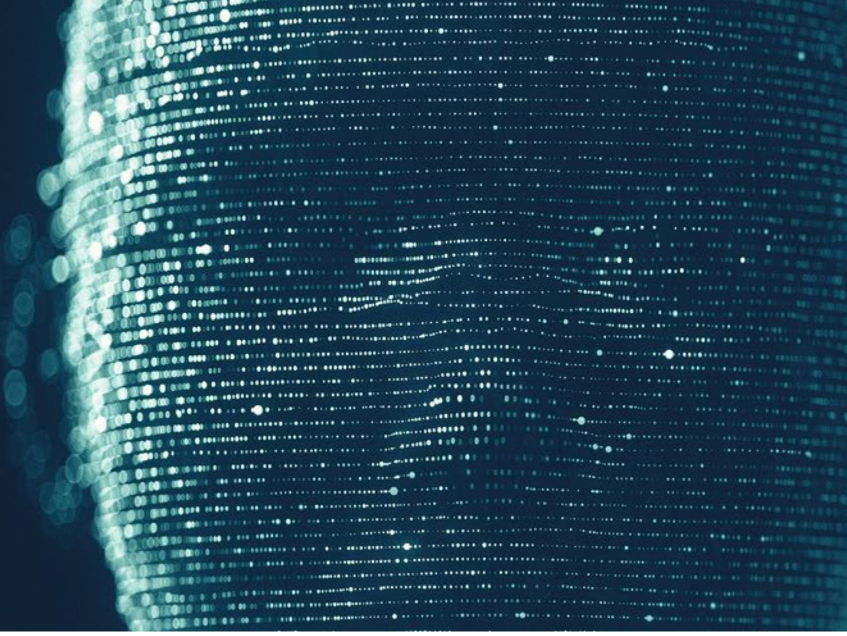
It's important to understand that AI will not remove the need for human operators. It will instead empower them with new tools that let them do their job more efficiently. The key is for security teams to consider how AI and ML models are trained with relevant data to not only provide correct information but also not disclose sensitive or regulated data. If the AI model lacks enough information, the answers delivered can often be biased, leading to mistakes and security risks in cybersecurity.

A strong Blue team of cybersecurity defenders should consist of skilled security specialists manning a SOC 24/7, empowered by modern security tools that utilize AI and ML to allow the security resources in your team to become as effective as possible.

Cybersecurity professionals need to continuously educate themselves to be able to not only stay on top of the latest developments but also discern which technology tools will best meet their needs.

An AI trained by senior analysts can assist a junior analyst in a SOC, helping them learn about investigation, reverse engineering, or threat hunting without any other resources, just learning with the tool. To some extent, this can address the shortage of competent personnel within the cybersecurity field.

In conclusion, rightly used AI can also help bolster our defenses, and cybersecurity companies like Truesec are also investing in AI research to offer even better protection in the future. Today, AI is far from capable of effectively being used alone for cyber attacks or defense. But when used intelligently, it can bolster the capacity of human operators on the defense, too.



Example:

The Deepfake CFO

The CFO of a multi-national corporation received a phone call from a person who started asking questions that seemed to be related to his position, but as the caller appeared to be a person of no interest, the CFO quickly ended the call. He didn't realize that he had already given the cybercriminals what they sought: a roughly 20-second recorded sample of his voice.

The cybercriminals fed this voice sample to a so-called deepfake voice generation tool. This tool allows the user to make voice calls and speak with the voice of the cloned voice sample.

Next, a series of phone calls were made to the financial departments in several subsidiaries of the corporation, in which the caller used deepfake voice generation to impersonate the CFO and tried convincing the personnel to transfer large sums of money to accounts under the control of the criminals, on the personal authorization of the CFO.

These fake phone calls were convincing enough to fool some of the staff, but luckily, most of the transfers were never carried out, as internal procedures required additional authorization for large money transfers. This is just one example of how cybercriminals and fraudsters are now beginning to use AI-driven deep fake technology to assist in social engineering attacks. Today, voice cloning is effective enough to fool people. Soon, similar technology will be able to fool the eye, too. So-called SIM swapping can even allow cybercriminals to make phone calls using the phone number of the person being impersonated.

In a world where we increasingly rely on cyberspace to contact each other, ensuring that we're talking to the person we think we're talking to and not a fraudster impersonating them is becoming increasingly critical.

While AI can be detected to spot deepfake AI, this will likely create a new spiral of "arms race." Ultimately, organizations must also implement procedures to guarantee that the caller is who they claim to be.

Efficient Cybersecurity

Challenge: Cybercrime Is Just Business

Cybercrime, in all its forms, is about cybercriminals exploiting weaknesses to make money. Cybercriminals make decisions based on business calculations. Your risk is thus directly proportional to your potential value to the attacker.

Cybercriminals evaluate their potential targets based on two criteria: how much effort it takes to compromise them and how much value they represent if the attack succeeds. The wealthier the target, the more effort a cybercriminal may be willing to spend to compromise it.

A bulk of automated attacks can be blocked by taking basic precautions; novice cybercriminals don't have the resources to buy expensive tools or access. Simply enabling MFA will be enough to stop many of these attacks. As these criminals rely on quantity to make a profit, the sophistication of each attack, time spent to scout the target, choice of specialized tools, social engineering, and even man hours tend to be limited.

The more advanced attacks, performed by a motivated attacker specifically targeting a particular organization, may still be partially due to opportunistic motives, such as exploitation of a known vulnerability, but the decision to spend time to exploit an initial breach and expand it until the environment is completely taken over, is motivated by the perceived value of the target. Most ransomware criminals evaluate their victims based on financial data, like annual turnover, cyber insurance, etc. Espionage groups base their efforts on stolen information's political and economic value.

A typical successful ransomware heist can net the criminals 2% of the victim's annual turnover in profit for a couple of weeks' work. If we can't make that unprofitable for the criminals by lowering their success rate, you can be sure the ransomware business will continue to grow.

Solution:

Protecting Your Digital Assets Is Protecting Your Business

"He who defends everything, defends nothing." – Frederick the Great

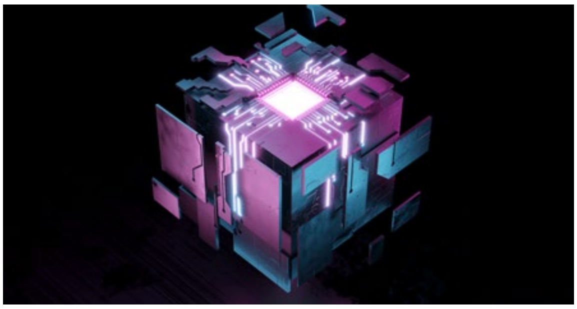
If you intend to abolish the risk of cyber outage by defending against any potential avenue of attack, you're likely to wind up spending a lot of money with relatively little effect.

So, what's the financial sector doing right that others can learn from?

The law of diminishing returns applies to cyber defense as well as to most other things: Protecting against the bulk of cyber attacks can be achieved through simple and cost-effective means. The more advanced the threat, the more costly it is to defend from.

Defending against cyber attacks should not aim to eliminate but to minimize risk. What risk you are willing to accept may vary depending on your business, geopolitical, and legal position. But cybercriminals are governed by business decisions. Your cybersecurity investments should be based on business decisions, too.

To determine adequate cybersecurity for your organization, you need to begin top-down with understanding your company's position in the current context of the threat landscape. That risk needs to be mirrored in your actual footprint and risk exposure. How is your business dependent on the internet? What exploitable attack surfaces does that expose? How would a serious cyber incident impact your business?



Ultimately, cyber risks will be translated into business risks. A ransomware attack can result in the loss of millions of euros in profit. Entire annual profits can be wiped out. Cybersecurity must be a part of your holistic risk management and a conscious part of your decision-making regarding IT infrastructure. It should have its own budget and governance but, at the same time, be a consideration in all aspects of your IT lifecycle, from process governance to target architecture and sunsetting.

Protect and Detect When Possible - Respond and Restore When Necessary

Protect
→
Detect
→
Respond

Protect

In order to **protect** effectively, you need to understand the viable threat – you need to predict the most probable attack vectors and attack motivations, the most probable targets, and your vulnerable assets. Is your business large enough to warrant the attention of an advanced ransomware group? Do you hold crucial intellectual property that could be valuable to foreign competition? Are you producing parts that can be used in defense technology?

The second step is to prevent attacks against these targets, focusing on threats you've identified as relevant to you, whether it's cybercrime, cyber espionage, or hacktivism. Ensure you understand your attack surface; what's exposed to the internet? Limit it and defend it using best practices. Ensure a sound, working, and fit-for-purpose patch management process that includes ANY system that is still online (whether sunset or not), taking special care with anything exposed to the internet.

Detect

Regularly ensure best practice aligned and correct configuration of cloud and other internet-facing assets, as well as keep a record of new and known vulnerabilities and how you can mitigate potential exploits of any existing vulnerabilities (including patch management, web application firewalls, etc.)

Ensure a modern strategy to **detect** and identify signs of attempted (and successful) breach. This should usually focus on endpoints (EDR) and AD assets (identities), which can then be further extended with NDR and, in some cases, SIEM. More advanced solutions may entail further XDR capabilities to protect specific cloud platforms, etc.

Ensure the platform is properly maintained and updated with detection rulesets capable of detecting malicious behavior – not only known indicators of compromise. Ensure that the analysts operating the platform are specialized in actual security alert investigation and that you have 24/7 capabilities active in front of screens.

Threat actors regularly practice avoiding your detection platform, and any more sophisticated attack should be expected to circumvent the most basic detections as well as be speedy enough to leave you minutes of reaction time to mitigate the impact. For the same reason, don't trust fully automated solutions; they're suited to counter only the most unsophisticated drive-by attempts, and a reasonably skilled human threat actor will know how to circumvent them. An EDR platform is NOT an automated antivirus and should not be treated as such.

Respond

Ensure that your detection layer maintains an immediate capability to **respond** to identified threats with force. Ensure process support for the isolation of individual endpoints in both the client and server layer; uphold rules of engagement to immediately address clear and obvious signs of a successful attacker entering the active phase (encryption or exfiltration). The bulk of this capability should reside fully integrated with your detection layer to ensure immediate response capability.

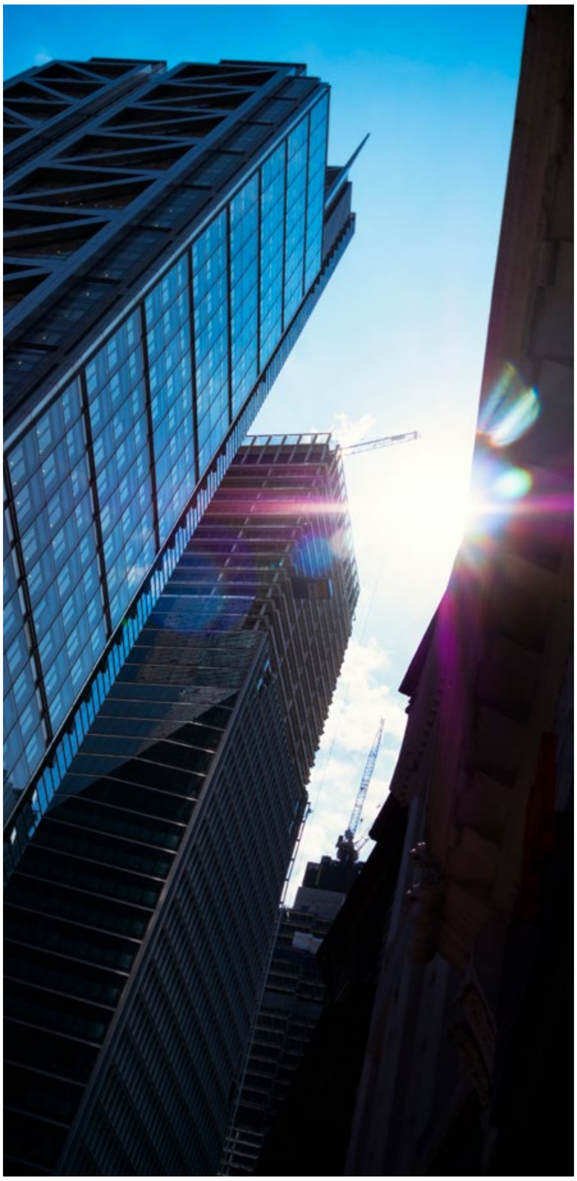
Maintain a philosophy of "Assume Breach"; expect that an attack can and will be successful – ensure that you have a specialized Cybersecurity Incident Response Team (CSIRT) available and fully integrated (prepared, practiced, and armed) with your Major Incident Management Team and processes. Understand that cyber breaches are not IT incidents; they must be managed differently. An active adversary will attempt to maximize their impact from the second you start your response; you need to minimize their impact on your business as well as ensure that you identify the full extent of damage (stolen or destroyed data or "just" encryption), that you eradicate any potential persistence, identify and close exploits and other kinds of malware.

The correct response to a cyber breach is more than just getting the business back in operation – it includes understanding how the compromise happened, what damage has been done, and how it can be avoided in the future. Threat actors can and will try to revisit the same target. Make that returning campaign costly and likely to fail.

Remember that the threat actors do what they do for a living every day. Make sure that your cybersecurity operations are staffed by people who are just as experienced,

and ensure a partnership with a dedicated organization that manages serious breaches daily.

If the worst comes to the worst, maintain a practiced, fit-for-purpose process and methodology to recover your business. A true disaster recovery capability: Ensure that restoration of data and infrastructure can be managed even if your AD is completely compromised and your entire environment needs to be rebuilt from scratch. Identify and plan for the successful restoration of critical systems and data stores. Practice with your CSIRT and IT operations provider. Disaster recovery from a successful cyber breach is no different from any other disaster recovery, but currently, it's by far the most likely reason for declaring a disaster – having long since passed by natural disasters, terror, and more.

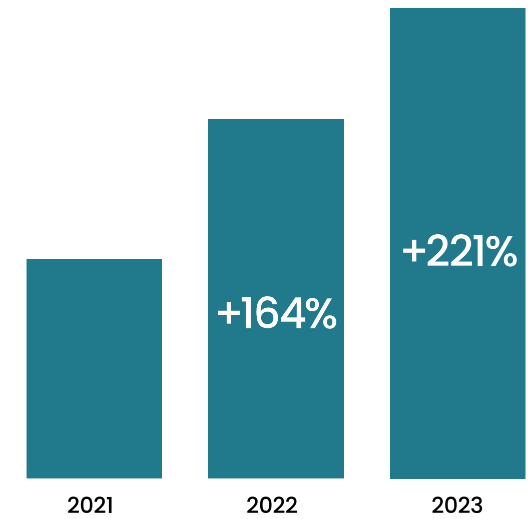


Example:

The Financial Sector in the Nordics

Below are some statistics for all serious intrusion attempts our SOC has prevented in the last three years. These numbers are normalized to how many endpoints we defend, so changes reflect real changes in the cyber threat landscape. We can observe how the number of intrusion attempts have increased to almost double the previous years.

Intrustion Attempts Disarmed per Monitored Endpoints Compared to 2021

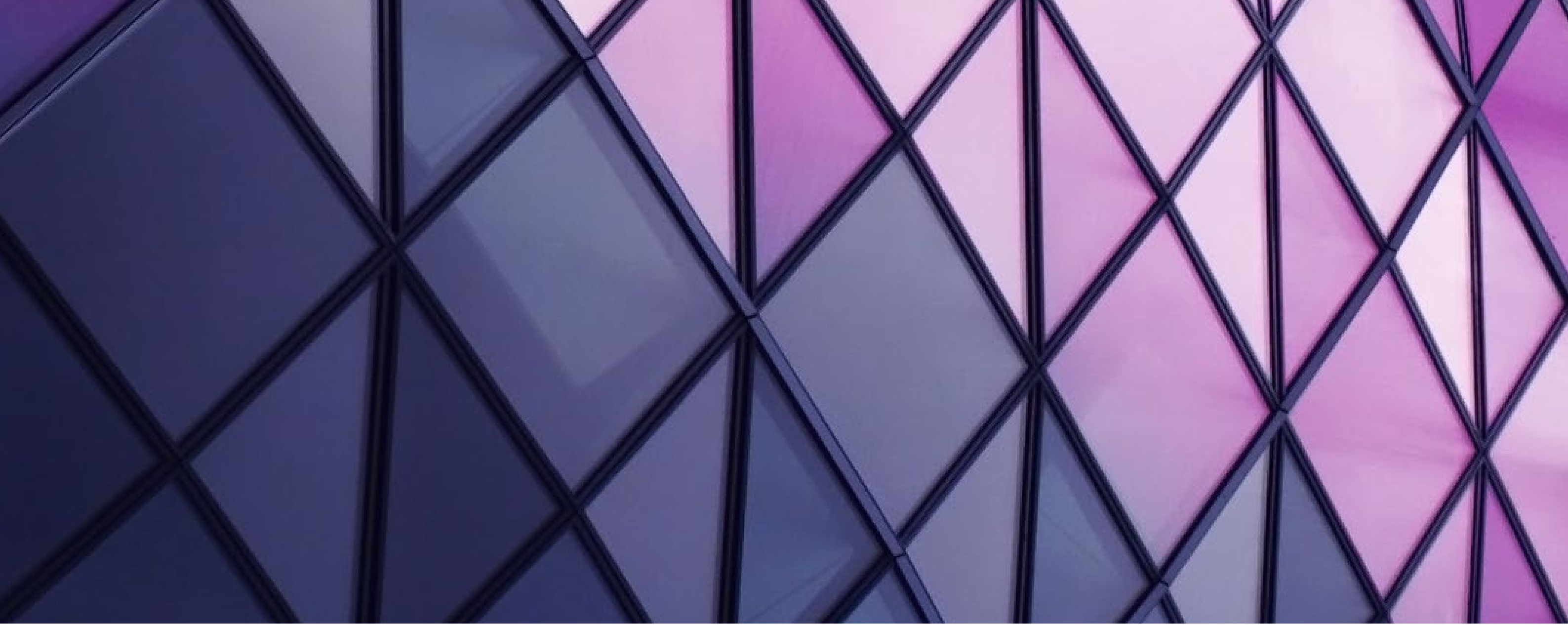


The most obvious change in threat actor behavior we've observed is an increase in automation and a general shift toward mass exploitation of known vulnerabilities.

Many large ransomware campaigns today begin with a threat actor that has written an exploit that allows them to compromise all unpatched machines with a particular software. They use online scanning databases to identify all vulnerable machines on the internet and run automated attacks to install backdoors on vulnerable systems. Then, they begin to pick them off, one by one.

Worth noting however is that when we isolate the financial industry in the Nordics, the numbers have not risen as in all other industries. There the number of intrusions prevented by our SOC against the financial industry remains in 2023 at roughly the same level as in 2021.

Traditionally, banks and other financial institutions are prime targets for all forms of crime. Banks represent everything that criminals want: money! This also applies to cybercrime, but when we look at the number of serious intrusion attempts we've stopped in our SOC in 2023, it's evident that there have been significantly fewer intrusion attempts against the financial industry than against other industries.



This highlights the opportunistic element of cybercrime. Organizations with good patch management will be targeted to a lesser extent than others because cybercriminals often gain foothold through exploiting vulnerabilities, and vulnerable systems can be found in online databases making the targeting fast and simple. Good preventive cybersecurity means drastically reducing the risk of your organization being targeted with a cyber attack.

The financial industry in the Nordics, and especially the major banks, have been leaders in cybersecurity, and our data shows that this has translated into fewer opportunistic intrusion attempts. No one should assume they're safe, but good preventive cybersecurity can minimize the number of attacks by cybercriminals, as they prefer easier targets.

New Laws and Regulations

Challenge: Knowing All New Legal Responsibilities

Being a leader – a CEO, senior management member, board member, etc. – is risky business. And with ambitious threat actors hunting for your organization's data – hungering for its money – and with legal responsibilities widening their scope, deepening their complexity, and placing liabilities on leaders personally, it's an ever-riskier business.

For example, legislators and regulators require organizations to keep track of their data and its inherent sensitivity; of processing-of-personal-data activities, including categories of data, data subjects, and potential risks; and of what technical, operational, and organizational measures are appropriate and proportionate to their determined aggregated risk exposure. These requirements are not, in and of themselves, new or, to be fair, unwarranted. However, they do require organizations to allocate resources from revenue-generating activities to "other" activities, or that's at least the sentiment in many organizations. They don't feel they have the legal maturity or the necessary resources to carry the costs related to cybersecurity compliance and data protection regulations.

At the same time, the laws and regulations related to cybersecurity and data protection (including privacy) have seen – and are seeing – rapid change. With these changes, the responsibilities placed on organizations and their leadership teams are also changing. A shared theme across all changes is that responsibilities are growing larger and more complex.

There is a shift of paradigms from "Comply or explain," where legislation allows organizations some leeway in how to fulfill the purpose of the legislation, via "Explain to comply," introduced with the GDPR, demanding organizations to document how they comply with the stipulated requirements to be deemed fully compliant; to "Prove to comply" introduced with NIS2, demanding compliance, documentation, and the ability to produce actual proof of how the organization complies with the legislation in its everyday business to be deemed compliant.

This shift to "Prove to comply" amplifies the onus that is put on senior management and leadership to ensure not only that their organizations comply with the legislative requirements but also to provide tangible evidence of such compliance. Another notable shift is the ever-extending downstream scope of responsibility in ensuring your organization's supply chains' level of compliance and

cybersecurity maturity. In other words, as a leader, you have the ultimate responsibility to ensure that your organization and supply hain live by the policies the organization has established.

An organization's security profile starts from the top with policies, procedures, and processes; these are the rule book for how the organization will work. This is where the procedures are established for the organization in accordance with the rules and regulations.

For example, it doesn't matter if you invest in a super secure high-end system if the implementation doesn't follow the security policies established by the organization. Yes, you have a shiny new thing that might prevent problems, but if the shiny new thing doesn't get configured, updated, or maintained in accordance with the policies, it might be a false sense of security.

Many organizations feel quite overwhelmed by all these regulations, and there's a clear desire among some to outsource all IT, assuming that the IT partner will be responsible for cybersecurity and compliance. Responsibility, however, can never be outsourced. The reality is that to be able to outsource IT in a way that is compliant with laws and regulations also requires knowledge of the same laws and regulations.

How do you ensure that everything in the organization is as it should be? Leaders are responsible for ensuring that an organization conforms to laws and regulations through policies, processes, and procedures.

Solution:

Don’t Shirk Your Responsibility

Having good cybersecurity has always been good business. The impact of a ransomware attack can cripple an enterprise both financially and reputationally. The only difference is that now it can also be against the law not to have proper cybersecurity when handling customers’ data.

To understand if you comply with data protection laws and regulations, it’s not enough to have proper policies in place. You also must ask yourself these questions:

- How, as a leader, can I make my organization understand and follow the policies we create?

- What do employees in the organization need to follow the policies?

- How do we as an organization measure the effect and compliance of the policies, laws, and regulations?

- How does the organization ensure that the policies’ goal is not just a one-time work but instead the DNA for how the organization does things?

- How do we transfer the meaning of our policies to our suppliers?

- What if we don’t do this work? How will the future of our organization look?

If you don’t have the cyber legal knowledge within your organization, you need to acquire it. You can’t always trust that the organization you outsource your IT to will act in your best interests.

Protecting Your Digital Assets

Challenge: When the Threat Actor Is Already Inside

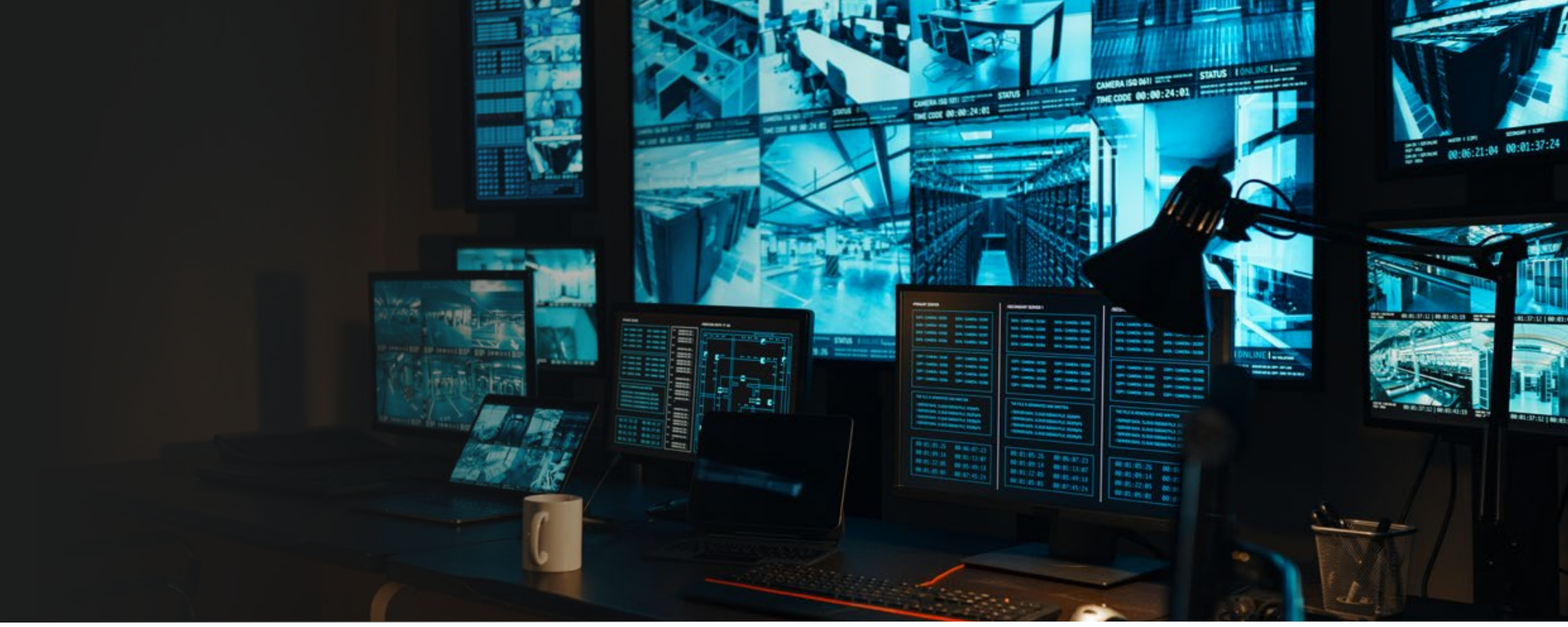
When your business is hit with a ransomware attack, and your digital assets are held for ransom, there's no avoiding the fact that your IT environment is, in fact, unavailable. You're left with no choice: the glove is thrown, and you must act immediately. Protecting your digital assets is about getting them back again. Your business is at a standstill until you regain control of your network.

The focus on ransomware and uptime sometimes steals the attention from other, more insidious threats. Many threat actors want long-term network access and do everything to stay undetected. They abuse their access to stealthily hijack information and abuse digital assets for their own purposes. These digital parasites can remain for years in your network, slowly feeding off your organization's hard work.

The theft of intellectual property is a well-known form of data theft. Despite how much has been written about cyber espionage, most organizations still don't understand how widespread the theft of intellectual property and information about tenders is. When a Chinese competitor wins a tender with an almost identical product, it's considered a business problem, not a cybersecurity problem.

In recent years, threat actors that steal information have become more and more refined, and we can rewind to February 2021, and the Exchange Server exploit attributed to the Chinese threat actor known as "Silk Typhoon." Truesec investigated a set of breaches where the threat actor gained access but wanted to stay undisturbed on the servers. To prevent other competitive threat actors from gaining access, the first threat actor updated the exchange server to prevent further breaches. By doing this, they could work undisturbed and move much slower, take a several months long pause in some cases, stay in the target environment, and figure out how to utilize the asset they now had at their disposal.

In 2023, the Truesec Incident Response Team has seen this taken to the next level, where the threat actor has not only gained access to a target environment but also established access of such sort that they now are a distributor of digital services (SaaS), from the target's environment, but through black market sales channels. The target environment gives information backend functionality, and the threat actor lives as a parasite of the "host body."



This year, advanced threat actors are increasingly abandoning the use of specialized malware and instead finding ways to abuse existing legitimate tools for hacking purposes. An advanced threat actor, low key, without utilizing known toolkits, only working with the tools already used by the customer, can stay undetected for years in an environment.

Another sometimes neglected aspect of protecting your digital assets is the insider threat. In 2023, Truesec has seen a rise in incidents involving various insider threats. The declining economy may have forced organizations to make painful decisions that leave employees disgruntled or disillusioned. Insider threats include:

- Employees with a risk profile that leaves them vulnerable to recruitment by threat actors.
- Failed off-boarding processes that leave an ex-employee disgruntled and angry.
- People leave for new opportunities, taking most of the old company IP with them.
- Self-appointed “whistleblowers” who try to exfiltrate data and expose what they consider bad practices.

Solution:

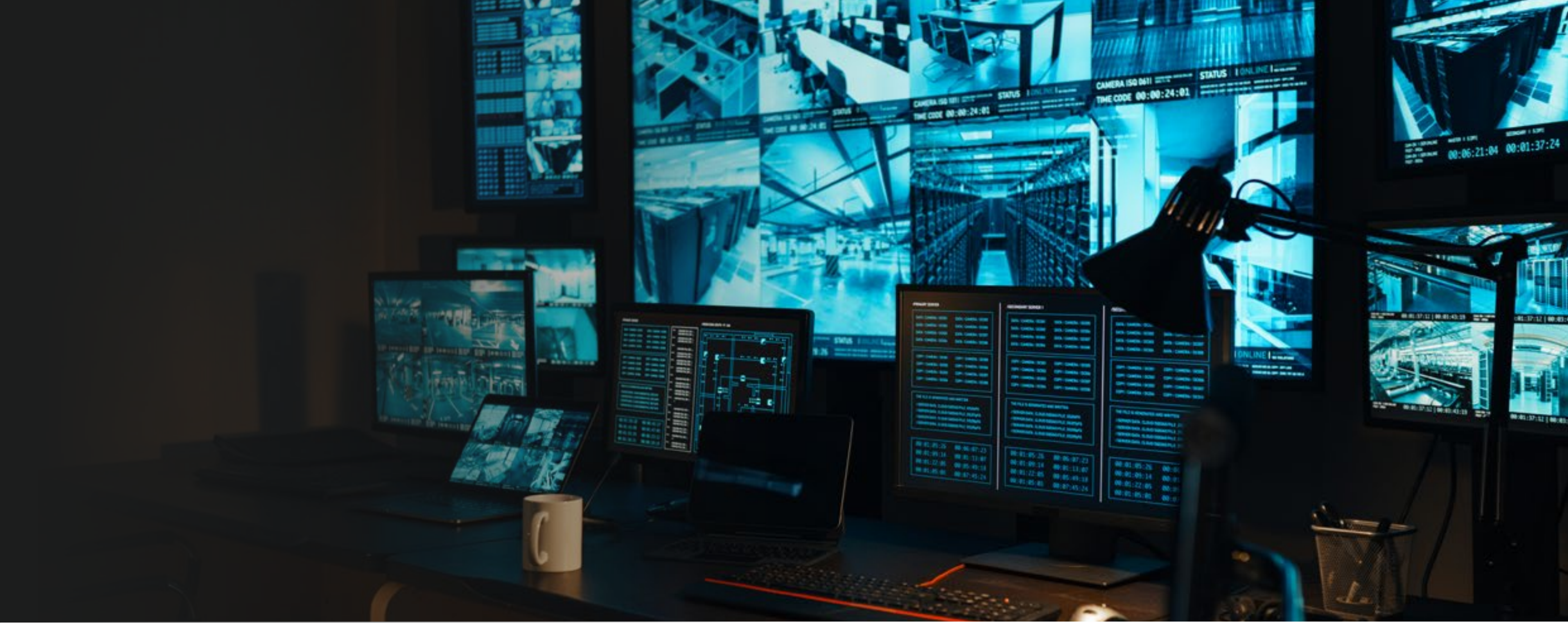
Incorporate Security in Your Architecture

Regardless of whether a threat actor managed to get into your systems from the outside or is an insider that already has access to your network, some key capabilities can enable you to detect and evict even a stealthy intruder that doesn't deploy any malware to steal data.

The challenges of investigating incidents involving stolen data are many and complex. Since everything is still running, there's no clear breaking point. The threat actor is not interested in creating havoc or chaos that would alert the victim to their presence. Everything is working, with the small caveat that a threat actor is now robbing the customer.

In these situations, pulling the internet cord and closing all VPN tunnels is not ideal. That action would, for real, cause chaos and havoc. That will affect businesses and customers. To succeed, an incident response team needs lots of logs, visibility, tools for containment, and a mandate to hunt and disarm the threat actor.

- Visibility is key. Extended detection and response (XDR) and a skilled detection organization that can find anomalies early.
- Identity management is crucial. Identities are always a top target for threat actors. Monitor and protect all identities.
- Maintain logs that make it possible for a Digital Forensic Specialist to analyze a long period of historical events.
- Prepare containment strategies in advance and ensure you can rapidly contain systems, applications, and network segments.
- A mandate for action will be needed, and awareness and preparations within the organization are of the highest importance.



The complexity of being able to correlate all log sources, knowledge gained from digital forensics, and a mandate that gives the threat hunters the ability to close, disable, and contain servers, clients, and networks requires a lot of expertise, but there's no alternative. Would you accept a robbery going on every day in your organization?

When it comes to insider threats, the best approach is proper security vetting of key personnel. Modern IT environments offer insiders the capacity to do untold damage if they have the right access and privileges. It's also important to remember that security vetting is not a one and done. Humans and their situation in life are constantly changing. People may lose their footing in life over things that happen to them unrelated to their work life, leaving them vulnerable to outside influence.

The person who would never dream of betraying your trust when they were hired can be in a different situation later in life. Vetting of key personnel should be a continuous program with recurring security checks.

Example:

When Your Digital Assets Become the Habitat for a Parasite

During a routine cybersecurity health check of a European manufacturing corporation, it was discovered that a threat actor was inside the network. The response team assumed that they had discovered a ransomware attack in progress. As the investigation continued, it was soon discovered that this threat actor had actually been inside the network for far longer than is typical for a ransomware attack – the earliest evidence of the threat actor being active in the environment dated almost two years back.

The forensic team decided that it was likely that the threat actor was not a cybercriminal but a state-sponsored espionage group. The skill and evasion technique used by the threat actor supported this theory. The threat actor relied entirely on living off-the-land binaries and techniques (LOLBins).

The threat actor managed to obtain full access to the directory, and persistence was ensured by cloning machines joined to the AD that were not in use. The threat actor had the AD under constant scrutiny and shifted clients it cloned as the need arose.

Evidence suggests the initial breach was the IT provider's jump server. This, in turn, indicates the attack was part of a much larger espionage campaign. It had all the markings of a broad cyber espionage campaign, like the Chinese Cloud Hopper attack.

When we delved into the threat actors' goals, we observed that the main focus of the threat actor's efforts appeared to be the software used in products made by the manufacturer. Like many manufacturers of advanced machines, their products included special industrial software. The threat actor's main focus appeared to be to continually exfiltrate the latest updated version of this software.

There is a market for such software. China is full of bootleg Western machinery. Sanctions against Russia mean that manufacturers won't allow updates to industrial software in Russia. Bootleg copies of the same software stolen by this threat actor are also for sale on the dark web.

Truesec can't definitively prove that the threat actor was a state-sponsored threat actor or for what nation they would have acted, but it's clear that proprietary software for popular modern industrial products is desirable enough to make an advanced threat actor go to great lengths to steal it. Like a parasite, they lodged themselves in the network to continually have access to the latest version of the software.

Predictive Intelligence: Our Outlook for 2024

Cybercrime Will Continue To Increase
In our 2023 Threat Intelligence Report, we forecasted that there would be a significant increase in ransomware due to Russia's ongoing isolation and the continuing deterioration of its economy. This prediction has come true, but perhaps at a slower pace than we initially anticipated.

Several factors prevent novice ransomware actors from quickly progressing into more advanced forms of ransomware attacks. Ransomware operators must be able to establish contacts in the ecosystem and have sufficient funds to invest in tools and access to reach the top tiers of organized cybercrime.

Top-tier ransomware syndicates prefer to target large enterprises that can afford to pay higher ransoms, but Truesec expects that even more ransomware groups will hit smaller enterprises next year. Many of the largest enterprises have improved their defenses and acquired effective managed detection and response capabilities. This makes them more difficult targets to breach, so all but the most experienced cybercriminals will move on to more accessible victims.

Some large enterprises still have vulnerabilities that expose them to ransomware, usually in the form of legacy systems deemed too expensive to replace. This still makes them "low-hanging fruit" for the ransomware criminals. However, just because cybercriminals are more likely to target smaller organizations doesn't mean that large enterprises can relax.

As the newer ransomware actors get absorbed into the established ransomware ecosystem, it's also likely that their skills will mature, as will their respect for the ecosystem's internal rules. Just as traditional organized crime is moving into cyberspace to conduct fraud or sell drugs, organized cybercrime will continue to adopt organizational structures reminiscent of real-world organized crime.

No Longer Looking for Malware
The most effective ransomware groups are now capable of obtaining and using zero-days, which are exploitable flaws in software that are, by definition, initially unknown to the rest of the world. When a threat actor has access to a zero-day that allows remote code execution, there's only so much defenders can do to stop the initial breach.
Both state actors and cybercriminals are also increasingly moving away from using specialized software and instead relying on abusing legitimate binaries. Using "living-off-the-land binaries" (LOLBins) or importing legitimate drivers with known vulnerabilities (BYOVD) to spread out in an environment means the threat actor no longer needs to bring malware that can trigger malware detection programs into the system.

Together, these two trends mean that it will be insufficient to base cyber defenses on detecting malicious code in the future. Instead, defenses must be based on detecting malicious behavior.

Breaking Out of Cyberspace
Russia is still the focus of the entire ransomware ecosystem, but in 2024, we'll likely see even more cybercriminals from other countries collaborate with the Russian ransomware syndicates. The risk of a significant influx of Western or Latin American hackers into the Russian cybercrime ecosystem cannot be overstated. Ultimately, Western law enforcement has a much better capacity to identify and arrest them.

The real problem with Russian cybercriminals recruiting Western affiliates isn't so much that they get in contact with Western hackers but that they may establish links to organized crime groups in the West capable of credible physical violence as an additional means of extortion.

Even here in the Nordics, some organized crime groups have begun to move part of their business into cyberspace, selling drugs on darknet marketplaces. Some of the organized crime groups in the Nordics are also capable of considerable violence. As organized crime increasingly moves into the darknet, they can establish more ties with cybercrime. Cybercriminals could, in the future, pay other criminals to make good on physical threats against victims who don't pay their ransom or even blackmail victims to give them access to networks.

In the future, identity management will likely be even more critical than it is now. Whoever has admin access to the entire corporate environment could, in the future, be a question of who needs physical protection.

The Future of Conflict

The more integrated our connected technology becomes, the more critical it is to protect it. Cybersecurity is more than just protecting networks; it's also about protecting society.

Even though the Russian cyber war in Ukraine has failed to deliver the kind of knock-out blow to the Ukrainian energy infrastructure they tried to achieve, there's no escaping that cyberspace is now an integral part of all modern conflicts. The West is sending more than armor and equipment to bolster Ukraine's defenses. Thousands of cybersecurity specialists are also helping Ukraine defend its networks.

Not only military conflicts but political and economic conflicts are now being fought in cyberspace: disinformation, fraud, theft of intellectual property, extortion, and false narratives. Cyberspace has become the primary battleground in the information war between freedom and dictatorship.

Mattias Wåhlén
Threat Intelligence Expert

Petter Fahlström
Chief Operating Officer MDR

Anders Näslund
Incident Manager

Daniel Olsson
Senior Enterprise Security Architect

Daniel Hesselberg
Head of Sales

Johan Ström
Senior Enterprise Security Architect

Levi Bergstedt
Chief Legal Officer

Daniel Jaurén
Head of Threat Intelligence

Mats Hultgren
Director of Operations IR

Marcus Murray
Founder

TRUESEC

www.truesec.com