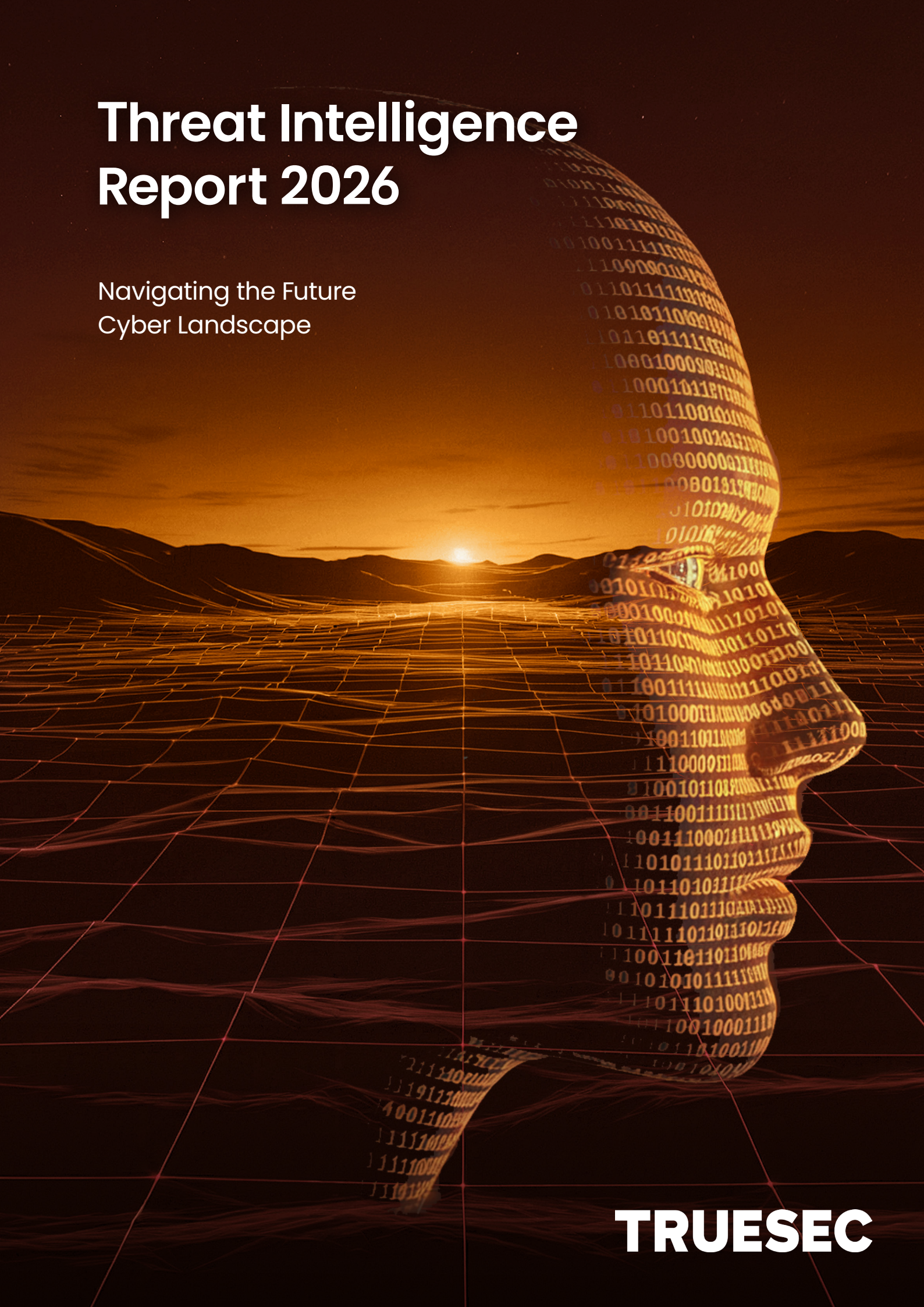
Threat Intelligence Report 2026

Navigating the Future Cyber Landscape



TRUESEC

A Message from Karin Hagman

The past year has shown how rapidly our world is shifting and how global tensions now directly influence the cyber threats facing organizations. State-sponsored activity is increasing; criminal groups are starting to use AI to scale out their operations, and the line between geopolitical conflict and cyber operations continues to fade. In this environment, the strategies that once worked are no longer enough. The threat landscape of 2026 requires new thinking, clearer priorities, and a deeper understanding of who may target your organization and why.

At Truesec, we witness these developments every day through our incident response, SOC operations and work and threat intelligence operations. This report brings together insights from our experts and from the Nordics' largest Security Operations Center to provide a clear, evidence-based view of today's threats and the actions that matter most in the year ahead. Our aim is not only to describe the threats, but to help you make informed, cost-effective decisions. To stay secure in 2026, organizations must strengthen resilience, invest in tools, services and processes that deliver the highest impact, and adapt their security posture to an increasingly complex environment.

Our mission is simple: prevent breaches and minimize the impact when they occur. Every day, we work to protect organizations and society from cyber-attacks, and we remain committed to being your trusted partner in this effort.

Thank you to everyone who contributed to this report,
and to you for taking the time to read it.



Karin Hagman
CEO, Truesec Group

About Truesec:

Truesec is a leading international cybersecurity company dedicated to preventing breaches and minimizing impact. We operate the largest SOC in the Nordics and have delivered over 120,000 hours of incident management. With 350+ specialists and AI-driven security capabilities, Truesec helps organizations across the private and public sectors strengthen their cyber resilience.

Learn more at truesec.com

Contents

About The Report 4
Acknowledgements 5
Executive Summary 6
The Threat Landscape **8**
The End Of Rules-Based Order 8
Conflicts In Cyberspace 9
Blurred Boundaries 10
The Globalization Of Cybercrime 10
The Fight Against Cybercrime 11
Cybercrime & Other Crime 15
Threat Actors & Their Motivators 18
Observations From Truesec **24**
Focus Areas **28**
The Constant Evolution Of Social Engineering 29
Threats From Within 34
When The Threat Doesn't Go Away 38
The Complexity Of Large And Multinational Organizations 44
Password Attacks Are Still Relevant 48
Malicious Packages Pose Software Supply Chain Risk 52
Deep Dive: The Malicious PDF Editor 56
The Use Of AI In Cyberattacks 62
The Challenge Of Knowing When "*The Regular*" Becomes A Threat 66
Not Taking The Regular For Granted 68
Hybrid Warfare **70**
Outlook 2026 **72**

TRUESEC

About the Report

Welcome to the seventh release of our annual Threat Intelligence Report. This report aims to contextualize cybersecurity trends and support defenders in their work to secure networks, prevent breaches, and minimize impact in a seemingly unpredictable world.

The first part of the report examines the current threat landscape, threat actors, and relevant cybercrime statistics derived from Truesec's engagements throughout 2025. The report then highlights a series of current cybersecurity challenges, supported by real-world examples observed by our SOC and CSIRT teams, and recommends solutions.

We conclude the report with our view of what we see on the horizon for 2026 and present our predictions in the Outlook section.

While examples are drawn from real-world experience, the case studies in this report are anonymized and sometimes an amalgamation of several incidents to protect client confidentiality. Our research encompasses a broad range of activities that generate data for our analysis. In addition to our own sources and accumulated knowledge from actual breaches and vulnerabilities, we also utilize information from private industry and law enforcement partnerships.

We are only as good as the work we deliver, and we appreciate any feedback you may have regarding this report. Please contact Truesec if you have any questions or comments.

Spokespersons:



Mike Clausen
Head of Threat Intelligence



Mattias Wåhlén
Snr. Threat Intelligence Expert



Mats Hultgren
Director of Cyber Risk



Petter Fahlström
Director of Operations

Acknowledgements:

This report is the result of the relentless and dedicated work of the Truesec Threat Intelligence team. Their deep understanding of the cyber threat landscape and threat actors, combined with extensive experience in intelligence collection, processing, analysis, and dissemination, has been essential to its development.

As much of their work necessarily takes place behind the scenes, we would like to take this opportunity to formally recognize and express our sincere appreciation for their expertise, professionalism, and continued commitment.

Karin Hagman
CEO Truesec Group

Rolf Rosenvinge
Chief Strategy Officer

Executive Summary

- Cybercrime is still the most prevalent cyber threat to most organizations, but it is not all about ransomware.
- Technology evolution, spearheaded by agentic AI, will change the game for both attackers and defenders.
- Cyberspace is a mirror of the geopolitical landscape. Cyber defenders need to prepare for a future in which Europe will increasingly have to find its own way, including in the cyber domain.

It appears that more organizations now have greater visibility into their environments and can acquire assistance to avert serious cyberattacks earlier in the kill chain. This has reduced the impact of many breaches. According to Truesec data, the total number of ransomware incidents in the Nordics in which a threat actor successfully encrypted victims decreased in 2025 compared with previous years. Instead, we have observed a corresponding increase in the number of incidents in which the threat actor was kicked out of the environment before reaching their final objective.

Initial attack vectors in breaches remain largely the same, even as the number of supply chain attacks has increased. At the same time, methods for establishing persistence within an environment have evolved. A majority of threat actors, both cybercriminals and cyber espionage groups, are no longer deploying hacking tools such as remote access trojans (RATs) or Cobalt Strike on victims' networks. Instead, they use commercially available remote management and monitoring (RMM) tools to ensure persistence. Various types of sideloading, hijacking, and the use of vulnerable drivers remain prevalent mechanisms across a wide range of attacks and steps within the kill chain.

Modern IT is full of integration and dependencies. Today, some of an organization's most sensitive data may reside outside the typical



network boundary. Threat actors are aware of this, and there are an increasing number of methods and attacks targeting web cookies and credentials stored in browsers used to access various software-as-a-service (SaaS) portals.

In 2026, Truesec expects more threat actors to incorporate large language models (LLMs) and other AI-based solutions into their attack chains. Skilled threat actors will use AI to automate tasks, making them cheaper and quicker to perform. This will not fundamentally change the challenge facing defenders, but it will likely necessitate faster responses. It can potentially also lead to a new wave of mass extortion attacks against smaller enterprises deemed unworthy of more targeted attacks.

The widespread adoption of AI will also make AI itself an attack surface. LLMs and other AI systems exposed to the internet will be targeted with prompt-injection attacks. In 2026, Truesec assesses that threat actors will start experimenting with using company LLMs to assist them in mapping their victims' environments, once they have gained a foothold. In 2026, your company's LLM could become the ultimate insider threat.

A key trend in the current threat landscape is the weakening of the international rules-based order. Since the end of World War II, the Western alliance has promoted a legal framework to manage global conflicts. Today, many of these established rules are being challenged, and their validity questioned. In this context, a robust and united European approach to cybersecurity is more crucial than ever. A key takeaway is that asymmetric conflicts shape the contemporary threat landscape. The armed invasion of Ukraine is met with financial sanctions from the West, which in turn triggers retaliation in the form of sabotage and disinformation. Regardless of the points of conflict between Europe and our adversaries, they will seek out our weakest spot. If cybersecurity is lacking, they will focus their efforts there.



The Threat Landscape

The End of the Rules-Based Order

A general theme for this threat landscape is the erosion of the international rules-based order. Since World War II, the Western alliance, led by the U.S., has advocated a rules-based order as a legal framework for managing international conflicts. Many of these rules are now being ignored with no consequences.

U.S. leadership of the Western alliance is eroding amid shifts in U.S. politics under the current administration. Rather than viewing the U.S.'s role as an unchallenged leader of the Western bloc and custodian of international regimes as a vital privilege to protect, the administration appears to see it as a power to be leveraged.

The effects of the U.S. administration's "America First" policies have influenced both national security and cybersecurity in Europe. Just as Europe has been forced to initiate a program of rearmament amid doubts about Trump's commitment to NATO, there are now also doubts about Europe's dependence on U.S. information technology.

Another problem with the U.S. administration's unpredictable leadership is that it undermines collective cybersecurity efforts. The U.S. Cybersecurity and Infrastructure Security Agency's (CISA) efforts to track Russian influence operations have reportedly been curtailed, and laws that promote collaboration between the U.S. government and private industry on cyber incidents have lapsed. Today, European nations are increasingly pressured by both the U.S. and China to align with these countries' respective positions on global conflicts, or face consequences.

As the international rules-based order crumbles, and there is a risk that international efforts against cyberattacks begin to fracture, adversaries like Russia, Iran, North Korea, and China appear to collaborate closer than ever, while the U.S. is increasingly acting on its own.



Conflicts in Cyberspace

The political and military alliance between Russia, Iran, and North Korea is also replicated in cybercrime. As North Korean soldiers fight under Russian command in Ukraine, and Iran supplies Russia with drone technology, North Korean and Iranian cybercriminals also collaborate with Russian ransomware groups.

The primary driver is the war in Ukraine. Russian society is under increasing pressure due to the costs of the war in Ukraine. Ukraine's campaign to target Russia's oil and gas industry is hurting Russia both financially and logistically.

One of Russia's main objectives is to isolate Ukraine by undermining the support from the West. The Russian strategy to achieve this is a combination of threats, sabotage, and disinformation. Russia invests significant sums in supporting extremist parties in Europe, both on the left and the right, to incentivize them to create strife and be openly critical of Ukraine. Russia also maintains a campaign of sabotage and other forms of pressure on Western allies to dissuade further support for Ukraine.

The geopolitical situation will determine the risk of cyber sabotage against Europe and its critical infrastructure. Today, international conflicts are often asymmetrical. The destruction of cables in the Baltic Sea, GPS jamming, drone disruptions, and DDoS attacks are all highly likely part of Russia's attempt to force Europe to end its support for Ukraine. At the same time, the West uses economic sanctions against Russia to force an end to its aggressive war.

Russia may raise the stakes and conduct more destructive attacks on critical infrastructure in Europe. In our chapter on Hybrid Warfare, we explore how this affects cybersecurity.



Blurred Boundaries

Another example of the erosion of the rules-based order is the blurring of the boundaries between state-sponsored cyber actors, private actors, and cybercriminals. Under pressure from the faltering war effort in Ukraine, the Russian government is increasingly leaning on criminal structures to support its efforts. Russian organized crime is enlisted to smuggle sanctioned items to Russia, while Russian cybercriminals breach networks or steal credentials and then sell the access to Russian intelligence agencies.

The collaboration between security services and criminals is almost always transactional, but the government doesn't always pay in money; it may also extort criminals by offering "protection" from being drafted into its cyber-espionage units or even being sent to the front. This suggests that Russian authorities, such as the Russian Federal Security Service (FSB), tolerate, guide, and potentially profit from ransomware actors.

While Russia's war in Ukraine dominates Europe's security threats, China is also a significant factor in Europe's cybersecurity. The commercial nature of much of China's cyber espionage also means that some private companies involved, engage in cybercrime. There are examples of Chinese threat actors linked to private companies that conduct cyber espionage for profit, and sometimes also engage in ransomware operations.

As boundaries blur and the rules-based order erodes, today's conflicts are increasingly asymmetric. An armed invasion is met with financial sanctions, which in turn trigger retaliation in the form of sabotage and disinformation. Regardless of the points of conflict between states and their adversaries, they will target their enemy's weakest spot. If our cybersecurity is lacking, then that is where our adversaries will strike.

The Globalization of Cybercrime

While organized cybercrime is a global problem, cybercrime has traditionally been divided into distinct regional ecosystems. Russia is home to much of the infrastructure used in ransomware. Western Africa is the center for an ecosystem of cyberfraud and business email compromise (BEC)[1]. Southeast Asia is the hub for so-called "pig slaughtering", fraud based on romance scams, and human trafficking.

As cybercrime matures, these ecosystems are increasingly merging, and cybercriminals from different parts of the world are collaborating more. Cybercriminals from Pakistan can sell phishing kits to Chinese cybercriminals in Africa or access brokers in Russia.

Geopolitical alliances are also duplicated in the cybercriminal world. North Korea's "Lazarus" group, a part of North Korea's military intelligence service, now collaborates with Russian ransomware groups to finance North Korea's program for weapons of mass destruction. At the same time, Iranian cyber espionage actors sell access to Russian cybercriminals for profit.

In recent years, Western cybercriminals, mainly from the U.S. and the UK, but also from France, Canada, and Brazil, have emerged

1. Read more about BEC in the Truesec Threat Intelligence Report 2025.

who conduct cyber extortion, sometimes in collaboration with Russian RaaS groups.

These hackers are often technically proficient and excel at various forms of social engineering, but they are often less professional in their business dealings than their Russian counterparts. Some of them also collaborate with Russian criminals and deliver ransomware from Russian ransomware syndicates in exchange for a share of the profits.

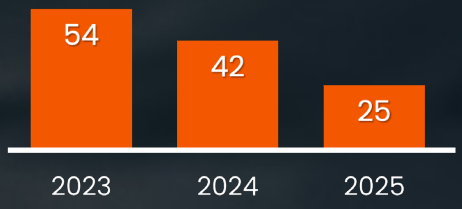
They belong to a loosely organized online collective known as "The Com," comprising young hackers driven by a toxic mixture of contempt for society and a desire for quick wealth and fame. They meet and radicalize one another in online spaces such as 4chan and Discord. They even recruit new members among young teenagers in game chat rooms such as Roblox and Minecraft.

As organized crime infiltrates society worldwide, cybercriminals are increasingly organizing on a global scale. While the ransomware ecosystem remains centered in Russia, it now includes cybercriminals from around the world.

The Fight Against Cybercrime

Both Truesec data and independent sources indicate that the number of severe ransomware attacks has declined since the 2023 peak, in both the Nordics and Northern Europe. The number of significant ransomware incidents has decreased by more than a third compared with earlier periods.

Latest Data from IR Cases



Even if we at Truesec see a decrease in ransomware attacks, independent sources show that ransomware attacks are still on the rise. One possible explanation is that many attacks that could have been classified as ransomware go undetected. Smaller and mid-sized companies are also more frequently targeted than large enterprises, adding to the number of unreported attacks.

Several factors may explain the decline in ransomware attacks observed in our data, with enhanced cybersecurity measures likely playing a significant role.

As our statistics show, more ransomware incidents are now discovered in time, before damage is done. A less savory possibility is that, as cybercriminals pivot toward easier targets with fewer defensive capabilities, they tend to attack smaller organizations, which may be more likely to "pay and move on," and thus are not represented in industry statistics.

Another reason may be that, despite political differences between the U.S. and the EU, there has been a successful international collaboration to capitalize on the fact that even if cybercriminals are often located outside the West, their IT infrastructure is often located in Europe or the U.S.

By analyzing the criminals' activities and identifying their servers, police can seize and disrupt the criminal infrastructure. Maintaining this collaboration is vital in combating cybercrime.

This year, several large ransomware-as-a-service (RaaS) groups and cybercriminal forums had their infrastructure seized by law enforcement. The continuation of this positive trend has disrupted activities by groups such as LockBit, Black Cat, and RansomHub, thereby fragmenting parts of the ransomware ecosystem.

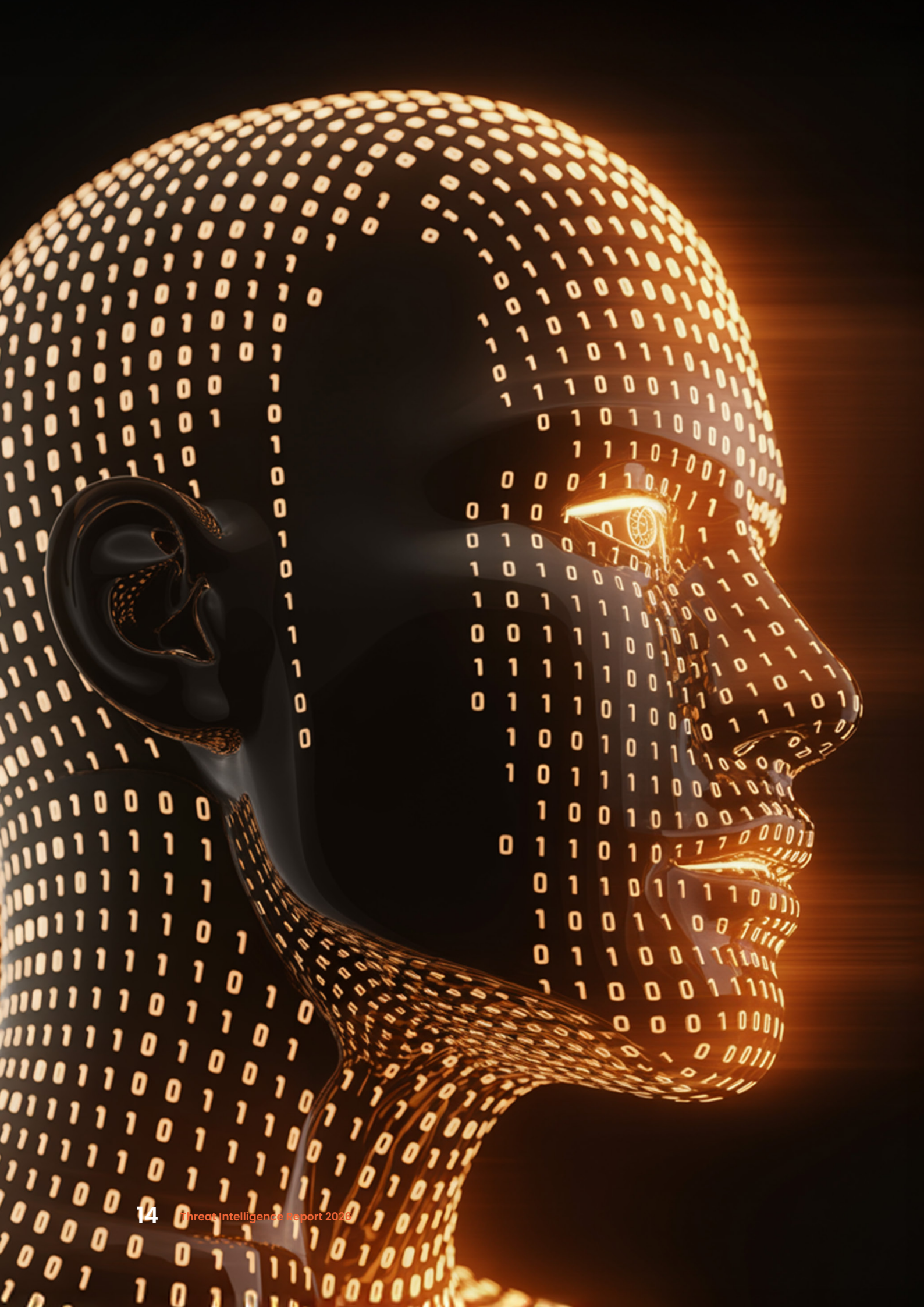
Truesec has seen more ransomware incidents that appear to have been conducted by small independent actors, either lone individuals or small teams, not connected to any of the large ransomware syndicates. Overall, this is still positive, as cybercriminals are almost always more effective when they organize and collaborate. At the same time, the cyber extortion ecosystem is resilient. Cybercriminals continue to trade information and services on various dark web forums. Newer RaaS brands, such as Qilin and DragonForce, have replaced older ones.

To truly impact cybercrime, cybercriminals must be arrested and sentenced, yet most still operate from countries that do not attempt to stop them. The conflict between Europe and Russia leaves little leverage for European nations to pressure Russia to act against cybercriminals, as the diplomatic arsenal is already almost exhausted.

Europe's diminishing influence in Africa could also lead to fewer opportunities for collaboration with local police. In 2024, over 1,000 cybercriminals and fraudsters were arrested in a joint INTERPOL and AFRIPOL operation. None of them came from a country where Russia supports the regime with mercenaries. If Europe's influence in Africa further deteriorates, there will likely be less collaboration to apprehend cybercriminals in the future. In our chapter, "The Complexity of Large Multinational Organizations," we look at how cybersecurity is affected by global threats.

The geopolitical situation always limits what can be achieved through international law enforcement. If European law enforcement is too successful in denying criminals access to inexpensive server capacity in Europe, they will likely relocate to other parts of the world, even if it is more expensive.





Cybercrime & Other Crime

Another trend is the fading of the boundaries between cyberspace and the physical world. Russian and Chinese intelligence agencies combine human intelligence gathering with cyber espionage. In Latin America, organized cybercrime is directly affiliated with drug cartels. Cybercriminals from Mexico steal personal information on government officials, hoping to find extortion material that can be used to protect the cartels.

An example of how physical threats and extortion have been used in conjunction with cyberattacks is a U.S. case in which an unknown cybercriminal hacked an individual's email account and identified their cryptocurrency assets. The threat actor then collaborated with a gang of criminals to stage a home invasion and, at gunpoint, forced the victim to transfer their cryptocurrency assets to an account under the cybercriminal's control.

In Sweden, Truesec has seen what we assess to be nation-state intelligence services using local criminals to target senior executives to get them to give up their organizations' support to Ukraine. It is possible that prior surveillance and intelligence gathering on these individuals was done through cyber-enabled means. Criminals for such actions are recruited through online forums and encrypted apps. A tactic that is also used by non-state aligned criminals to recruit children and young adults to carry out violence on behalf of organized crime, highlighting the link to cyberspace and the disintegration of national borders. Actions in the cyber domain enable crime and terrorism in the physical domain.

Even if it's still relatively uncommon that cyberattacks are seen in combination with physical violence, communities like the online collective known as "The Com" have members that conduct cybercrime, but also members that offer swatting-as-a-service[2] and violence-as-a-service. However, the overwhelming majority of the violence-as-a-service offerings found on the darknet today are likely still fraudsters. While this is the case, we do see an increase in the solicitation of criminals through online forums and encrypted apps to carry out violence on behalf of malicious organizations.

2 Threat actors coordinate fake emergency calls by spoofing phone numbers and using compromised smart devices to make the fake emergency seem to come from the victim's home, enhancing credibility with 911 dispatchers. The goal is to draw heavy police response (SWAT teams) to the location, creating chaos, and to distract law enforcement while committing other crimes, like crypto theft.

New Technical Challenges

A trend that has persisted since 2024 is that threat actors have sought to minimize their use of custom-made hacking tools on the victim networks to avoid detection.

Most threat actors, both cyber-criminals and cyber espionage groups, are no longer deploying hacking tools such as RATs or Cobalt Strike on victims' networks. Instead, they use commercially available RMM tools, such as TeamViewer or AnyDesk, to establish persistence. The only major exceptions are RATs introduced via malicious code packages from code-sharing sites.

By using commercially available tools and only running hacking tools remotely on their own machines via VPN connections, they avoid downloading any files that could be flagged as malicious on the victim's network or directly exposing the attacker's infrastructure.

Threat actors also often abuse old, but legitimate, drivers that are vulnerable to exploitation. They exploit the drivers' high privileges to disable security applications such as antivirus and EDR agents. Various types of sideloading, hijacking, and the use of vulnerable drivers remain prevalent mechanisms in a wide range of attacks and steps within the kill chain.

The introduction of LLMs and other AI will add new tools to the threat actor's arsenal. In our chapter on The Use of AI in Cyberattacks, we examine how AI will alter the threat landscape and what will remain the same.

Some threat actors are now experimenting with blockchain technology to hide command-and-control communications within "Smart Contracts". Malware retrieves encrypted C2 details from smart contracts through blockchain calls, decrypts the payload in memory, and initiates contact, all while blending in with legitimate blockchain traffic.

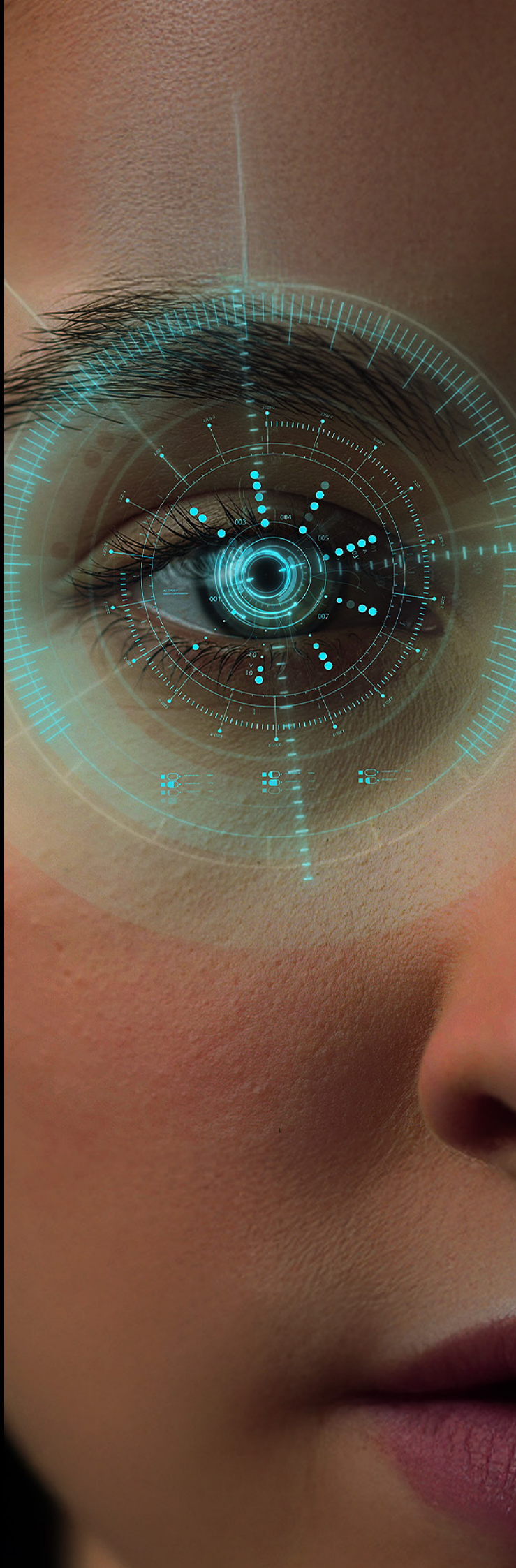
Overall, threat actors are adept at identifying and compromising high-privilege accounts.

This is typically because many organizations still have administrators using high-privilege accounts for everything, rather than only for work that requires them, which makes it easy to find. In our chapter, "Malicious Packages Pose Software Supply Chain Risks," , we examine in greater detail how threat actors are now targeting software developers with high privileges.

Modern IT is full of integration and dependencies. All this means that the boundaries of your environment get increasingly blurred. Today, some of an organization's most sensitive data may reside outside of a typical network boundary.

SaaS, or even more sensitive, than what is present on the typical user's devices. The threat actors know this, and there are an increasing number of methods and attacks targeting web cookies and credentials stored in browsers.

There is now also a whole ecosystem of log sellers, cybercriminals that buy and sell stolen data from various cyber breaches and information-stealing malware, and store it in large searchable databases. In our chapter, "When the Threat Doesn't Go Away," we examine how stolen data can be remonetized in new cyberattacks..



Threat Actors & Their Motivations

In the cybersecurity landscape, the term threat actor encompasses a diverse array of individuals and groups. These range from nation-state operatives and organized cybercriminals to hacktivists and insider threats. These actors don't operate in neat, isolated categories; instead, their techniques, tactics, and procedures frequently overlap, creating a complex and often confusing environment for defenders. The boundaries between different threat actor types are increasingly blurred as tools and methods are shared, sold, or copied across the underground ecosystem. This makes clear-cut attribution challenging. What matters most today is understanding how threat actors operate, what motivates them and how current events shape their actions, but most importantly, how these actions impact organizations. By focusing on behaviors and intent, defenders can better anticipate and respond to the evolving threat landscape, regardless of who is behind the keyboard.

Intelligence Agencies

Government hackers employed by intelligence agencies primarily conduct state-sponsored cyber espionage. They are controlled by the executive power of their respective nations, and their tasks are primarily tied to national security. Their ultimate goal is to ensure the survival of the nation or the regime and to support national security objectives, potentially including surveillance of perceived internal threats in non-democratic nations.

Typically, in Western democracies, national cyber espionage assets are limited to protecting democracy and to strictly defined national objectives. In authoritarian countries, government cyber espionage is tasked with protecting the current regime's safety, perpetuation, and finances. This means that countries like Russia, China, and Iran all use cyber espionage and cyberattacks against their internal and foreign political opposition.

The escalating global trade war has also helped fuel cyber espionage. Both the U.S. and China view global research and trade from a conflict perspective, in which gaining the upper hand over adversaries is as important, if not more so, than pursuing mutually beneficial solutions. This leaves little room for other nations to avoid being drawn in.

Cyber espionage is also tasked to support national agendas in trade conflicts. China has long been the most active nation in industrial espionage. China conducts extensive cyber espionage against Western enterprises and research centers to favor Chinese industry, as the regime in China considers this vital to fulfill its national security objectives.

Both Russia and Iran conduct cyber espionage on actors in the oil and gas market and government actors involved in sanctions regimes. Since the sanctions against Russia following the invasion of Ukraine, Russia has also attempted to steal information that can support its domestic arms production. Iran, Russia, and North Korea also use cyber espionage to circumvent international sanctions on specific technologies. For example, threat actors have been observed attempting to hack companies involved in missile and nuclear technologies to establish domestic production of sanctioned technologies.

Both the U.S. and China are also assessed as using their dominance in software (the U.S.) and hardware (China) to gather information on their adversaries. In our chapter, "Securing Your Data in an Insecure World," we examine in greater detail how to address these challenges.

Private Cyber Actors

In addition to government actors, a growing number of private corporations conduct cyber espionage for profit. These so-called private sector offensive actors (PSOAs) are essentially cyber mercenaries.

Many of them have residences in jurisdictions with permissive local legislation, primarily in Israel, but also in Italy, Switzerland, and India. Governments often employ these actors in nations that lack their own national cyber capabilities, and also in regimes that secretly seek to use them against the opposition in their countries, circumventing legal restrictions on government espionage. In 2025, a spy scandal in Italy, involving a large Israeli PSOA, was revealed.

China has a large ecosystem of private IT and cybersecurity companies that conduct cyber espionage on behalf of the Chinese government for payment. Most appear to be linked to the various provincial headquarters of China's security service (MSS), but these ties are often transactional. Successful companies are likely rewarded with access to zero-days that the government is actively hunting.

The Chinese example demonstrates that PSOAs ultimately prioritize profit, even when serving customers in the pursuit of national security objectives. Another example is an Indian PSOA that sells their services to both the Indian government and private companies engaged in costly litigation.

Organized Cybercrime

All organized crime, including cybercrime, is essentially driven by two goals: making money and avoiding arrest. The lower the risk of detection, the more business-like the activity becomes.

It's a well-known fact that Russia has an extensive ecosystem of organized cybercrime that the Russian government tolerates. Cyber extortionists research their victims' economic activity and annual turnover before setting the ransom amount. Sometimes they even steal information about the victim's cyber insurance before they set their demands.

Cyber extortion typically involves ransomware, data-leak extortion, or both. Data leak extortion is most effective against victims who hold sensitive client information. Private healthcare and law firms are typical victims of data-leak extortion, whereas the manufacturing industry is immediately affected by ransomware if production stops.

Organized cybercrime thrives in regions characterized by corruption, a weak rule of law, and widespread distrust of the ability to succeed by playing by the rules. What sets organized cybercrime apart from other forms of organized crime is its borderless nature. It's possible to conduct cybercrime in Europe, even if you are physically sitting somewhere on the other side of the world, out of reach of European law enforcement.

Africa, particularly Western Africa, has an extensive ecosystem of cybercriminals specializing in various forms of cyber fraud. These range from simple "Nigerian Prince" email fraud to more advanced cyber-enabled fraud, known as BEC. There are also signs that Chinese cybercriminals are beginning to establish themselves in Africa, exploiting the weak rule of law and China's regional influence.

As a rule, cybercriminals attempt to protect their anonymity as much as possible. Even if Russian cybercriminals are seldom arrested, the power balance between them and the government changes to their detriment if their identities are exposed by Western law enforcement.





Hacktivists

Politically and ideologically motivated cyber threat actors, so-called hacktivists, have traditionally been part of an internet counterculture. Nowadays, the term has been hijacked and used as a masquerading technique by a mix of threat actors that share the same tools and messaging tactics. In both cases, the label "hacktivist" is misleading.

State-sponsored threat actors can pose as "hacktivists" to create deniability for their actions. These actors are essentially cyber units that conduct hybrid warfare in cyberspace. They are often funded directly by an intelligence agency.

Private actors are often motivated by financial objectives. These "hacktivists" often cultivate online followers and try to solicit funds from them. Their business model is like that of YouTube and Twitch influencers. Some of these actors use their hacktivism to advertise commercial DDoS services. Overall, the DDoS ecosystem has evolved into a criminal industry, in which few genuine hacktivists can afford to participate unless they adopt a crowdsourcing business model.

There is considerable collaboration between these two groups, especially in Russia. Private actors seek collaboration with state actors, as they have access to funding and better tools, while state actors can use links to private actors to obscure their origins.

Both types of hacktivists rely on fear, uncertainty, and doubt (FUD) rather than actual impact. State-sponsored hacktivists seek to instill fear and maximize the political impact of their attacks, without crossing the line into physical damage on a scale that could provoke retaliation. In contrast, private actors often seek to amplify the perceived impact of their attacks among followers to solicit funding.

The closest to real "hacktivists" in the original sense are now mostly in low-cybersecurity third-world countries, where lone hackers with moderate skill can still affect websites. Such hacktivists often employ web defacement, hacking a website and redirecting it to an image that defames the website owner, as their preferred tactic.



OBSERVATIONS FROM

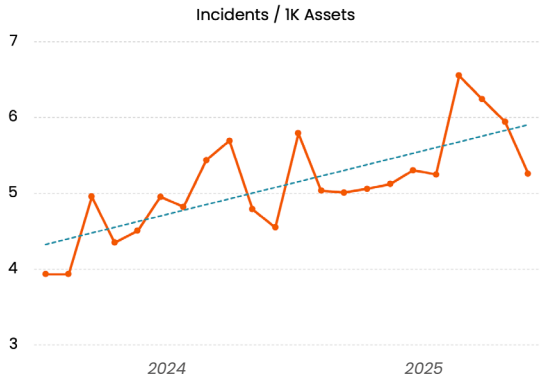
TRUESEC

01010100 01010010
01010101 01000101 01010011
01000101 01000011



Most of the incidents Truesec has handled have been carried out by cybercriminals motivated by financial gain. Cybercriminals use extortion or fraud to obtain money from victims or to gain access to sell it to other criminals.

By measuring the number of intrusion attempts averted in Truesec SOC each month and normalizing it to the total number of endpoints protected, a rough estimate of the cyber threats can be obtained. This data shows that the number of attempted cyberattacks is increasing steadily.



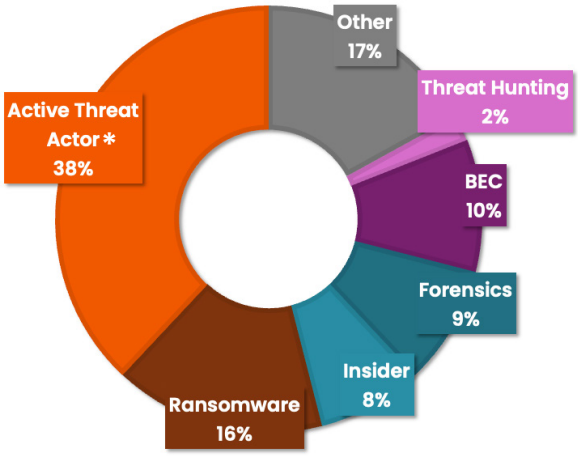
In our last Annual Report, we noted a decline in the number of serious ransomware incidents targeting large enterprises in the Nordics, as cybercriminals shifted their focus to smaller organizations.

In our Truesec data, we see that this trend in ransomware continued in 2025. The total number of ransomware incidents in which a threat actor successfully encrypted and extorted victims has decreased. In contrast, we observed a corresponding increase in incidents in which the threat actor was kicked out of the environment before reaching their final objective.

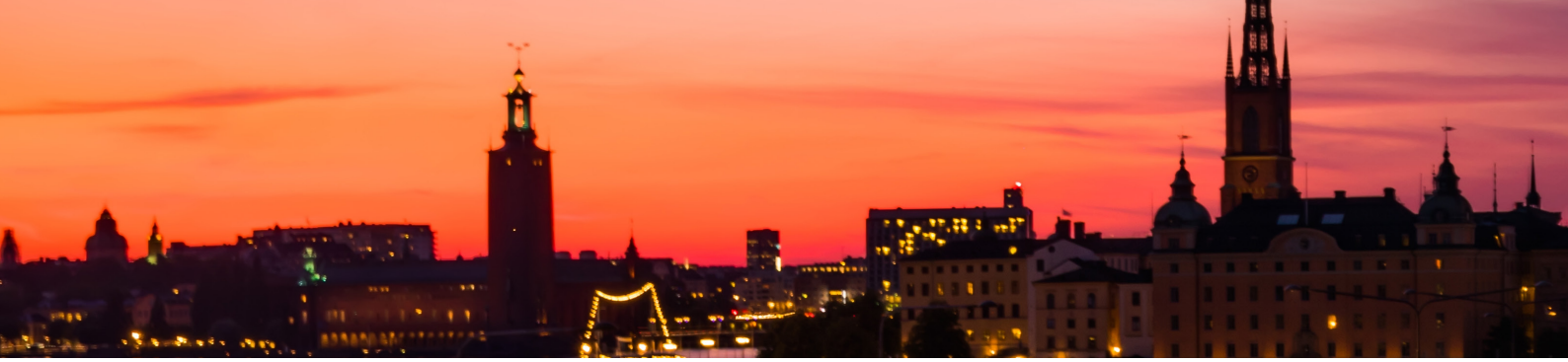
It appears that more organizations now have better visibility into their environments and can request assistance earlier in the kill chain to avert serious cyberattacks, such as ransomware, reducing their impact. This highlights the importance of proper detection and response capabilities.

There are just as many serious cyberattacks as last year, but with better detection, fewer have escalated to the worst outcomes.

Distribution of the Origins of Incidents Handled by Truesec CSIRT in 2025



**Active threat actor refers to incidents where the threat actors are contained at such an early stage that their ultimate objectives could not be determined.*

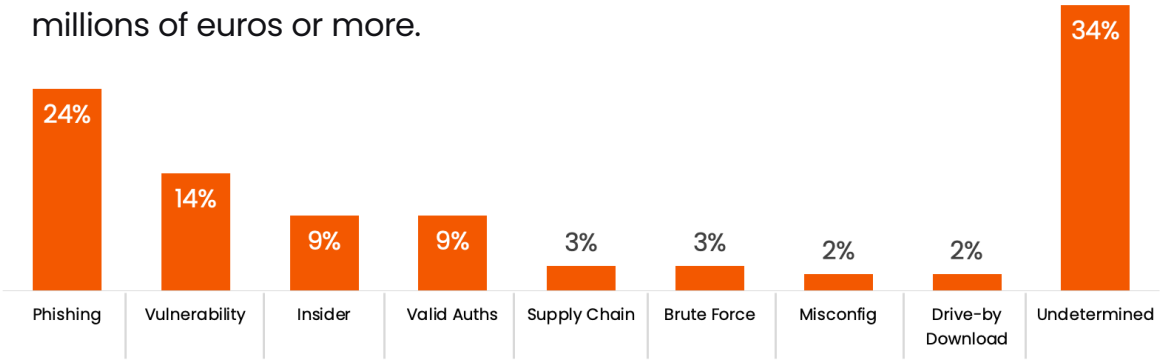


We can also see the effects of international law enforcement's disruption campaigns on the RaaS model during 2025. The relative number of incidents attributed to affiliates of one of the many RaaS groups has decreased compared with 2024, and more ransomware operators now prefer to operate alone or in small groups, without relying on a RaaS as a partner. This also makes them less effective, as only large groups can afford to update their ransomware regularly, while smaller operators often must rely on leaked binaries from older ransomware types.

A form of cybercrime that has risen during 2024 is BEC. BEC occurs when a threat actor hacks a corporate email account and sends a fraudulent email in the account owner's name, attempting to lure the recipient into transferring funds to accounts under their control. By hijacking business transactions, such attacks can result in losses of millions of euros or more.

Truesec CSIRT also has data on initial attack vectors used in successful cyber breaches. Phishing remains the most common attack vector across all types of attacks, even if the trend is falling. That said, phishing is rarely the initial attack vector in ransomware attacks. Ransomware attacks typically begin either with credential-based attacks (password spraying or compromised credentials) or by exploiting vulnerabilities in some internet-exposed applications, usually a VPN, firewall, or other security product. In our chapter, "Password Attacks Are Still Relevant," we take a deeper look at credential-based attacks.

BEC attacks, on the other hand, are almost exclusively carried out via phishing emails, as the entire attack chain aims to compromise email accounts.



Distribution of Initial Attack Vectors in Incidents Handled by Truesec CSIRT in 2025
Undetermined: Cases where the root cause could not be confidently established due to insufficient or compromised evidence.



As shown in the statistics, supply chain attacks are becoming increasingly common, although they remain relatively rare. However, there is likely a particular bias in this data. Typically, it is the company directly affected by a cyberattack that contacts an incident response company, not its customers or partners, who would consider the same incident a supply chain attack. This includes victims impacted by downloading malicious packages.

The rise in drive-by download attacks is fueled by a recent uptick in so-called pastejacking or “ClickFix” attacks, in which threat actors compromise legitimate websites to display a fake CAPTCHA page that prompts users to copy and paste code into their terminal to prove they are human. In our chapter, "The Constant Evolution of Social Engineering," we examine various social engineering threats in greater depth.

Truesec data reveals that, on average, the time from the first time a human operator is active in the network to full encryption is now slightly faster than it was a few years ago.

Time	2022	2025
<1 Day	12%	29%
<1 Week	59%	50%
>1 Week	41%	21%

Table: Time from First Action on Victim to Full Compromise

We can also measure the size of the victim organizations and see that a larger percentage of victims are smaller organizations than in previous years.

Size	2023	2024	2025
1-50	24%	15%	50%
51-500	25%	37%	29%
501-5K	34%	30%	17%
5k+	17%	18%	4%

Table: Percentage of Ransomware Victims compared to Company Size as Numbers of Employees

Comparing the last two tables suggests that the primary reason for the faster ransomware attacks is that more victims are now relatively small organizations, with smaller environments that are quicker to compromise.



Focus Areas

The Constant Evolution of Social Engineering

From Help Desk to Extortion

In 2025, Truesec assisted a company that experienced a serious cyber-extortion incident that began not with a phishing email but with hundreds of seemingly pointless spam emails. Social engineering takes many forms, and threat actors continually devise new tactics to exploit the human mind to achieve their objectives.

This time, the access method was a relatively new technique known as "BazarCall," also referred to as "callback phishing." It's particularly challenging as it requires no breach or system access to initiate; the only thing the attackers need is your email address.

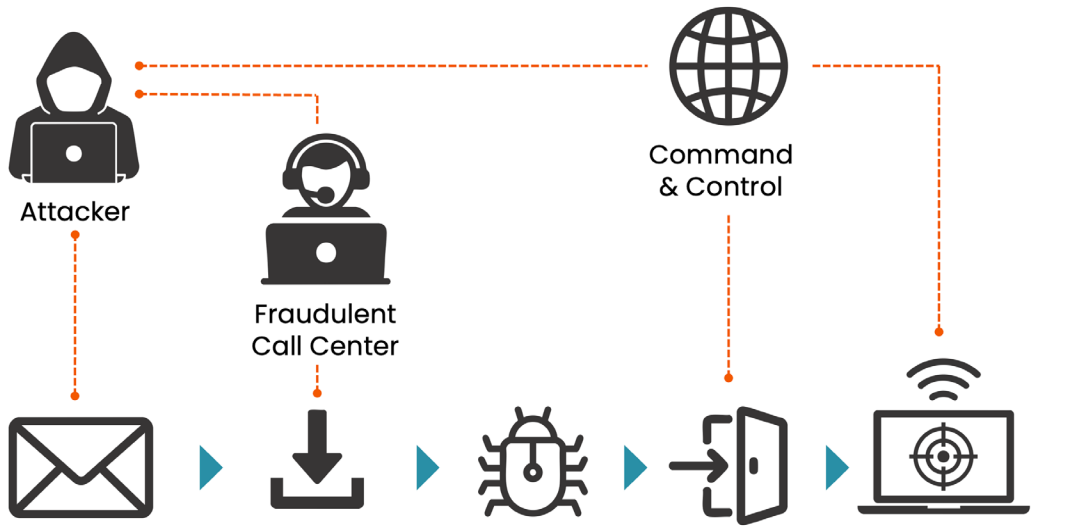
The threat actor known as "Silent Ransom" began by identifying valid email addresses of several employees at their chosen targets. We don't know exactly how, but finding valid corporate email addresses is easily done using open source intelligence (OSINT) techniques, which sometimes is as simple as checking the company's website or social media.

Their next step was to register email addresses for numerous subscriptions to various newsletters, websites, and other services eager to expand their mailing lists.

This resulted in hundreds of emails flooding the victims' inboxes, causing them significant stress as they were caught completely off guard.

What was once a manageable stream of messages became an overwhelming deluge, turning routine communication into chaos. This tactic not only disrupts productivity but also significantly increases the difficulty of locating legitimate, important, and time-sensitive emails.

This creates a twofold effect: first, it reduces the likelihood that the user will notice legitimate assistance from IT or security teams, while



simultaneously generating a sense of urgency to resolve the issue. At this point, the threat actor stepped in, positioning themselves as the solution to the problem they had created.

The threat actor created a fake Microsoft Teams account using a typo-squatted domain and posed as an internal help desk representative familiar with the victims' issues. Initially, they sent chat messages. If the victim ignores these messages, the attacker escalates by initiating a Teams call to add pressure and increase the likelihood of engagement.

The stress and confusion caused by hundreds of unsolicited emails made the attacker's offer of help seem almost irresistible. The victim, eager to resolve the issue, became highly susceptible to social engineering. To "fix" the problem, the attacker claimed they needed access and tricked the victim into activating Quick Assist, a built-in Windows feature for remote access.

Its presence in the operating system added a layer of perceived legitimacy, allowing the attacker to instruct the victim to use a "trusted and approved" tool without requiring any downloads or installations. This tactic significantly lowers suspicion and increases the likelihood of compromise.

At this point, the threat actor gained complete control of the victim's computer. They installed a commercial RMM tool to maintain persistence, then enumerated the environment and located sensitive data they downloaded to a service under their control. They finished by sending an extortion note.

The Silent Ransom group specializes in data-leak extortion rather than deploying ransomware. They target organizations that hold large amounts of sensitive customer data, such as legal services, insurance agencies, and private healthcare providers, and rely on the fear of business impact if the victim's customers learn that their data has been lost to coerce victims into paying.

Why Hacking Humans Remains a Challenge

As organizations continue to invest in technical cybersecurity measures and overall industry maturity rises, a significant shift has been observed in the methods employed by threat actors. Truesec has noted that while technical vulnerabilities remain a concern, attackers also exploit human vulnerabilities. Even the most advanced systems can be bypassed when an attacker successfully manipulates a human, often considered the weakest link in the security chain.

Western organizations operate on a foundation of trust, openness, and collaboration. However, this consequently creates an environment that malicious actors can exploit. A high-trust culture may lead employees to respond quickly to perceived

authority figures or overlook inconsistencies in requests that appear to originate from internal sources. Attackers are increasingly manipulating this cultural predisposition toward trust and cooperation to gain initial access.

In pursuit of human exploitation, threat actors deploy a range of techniques, including phishing, impersonation, and pretexting[3] as the initial attack vectors for broader compromise; of these, phishing remains the most prevalent. These techniques have evolved significantly through the integration of advanced AI capabilities, such as deepfake technology, which allows the creation of realistic voices or video impersonations. Such advancements blur the line between genuine and falsified communication, making detection increasingly difficult even for trained individuals.

Social engineers rely on well-documented psychological principles that influence human decision making, such as authority, urgency, reciprocity, social proof, and scarcity. These principles manipulate individuals' emotional responses and cognitive shortcuts, leading them to act without thoroughly assessing the legitimacy of a request. For example, an attacker posing as a senior executive may exploit authority to pressure an employee into executing a financial transaction. At the same time, a fabricated security alert may create a sense of urgency that elicits immediate action. In this context, the attacker's success depends less on technical sophistication and more on the ability to predict and exploit human tendencies.

The targets of social engineering are not confined to specific departments or hierarchical levels. Attackers may target IT personnel, developers, and executive leadership, as well as employees in administrative, financial, or customer-facing roles.

Even individuals without privileged access can be manipulated to provide small pieces of information that, when aggregated, enable a larger intrusion. This demonstrates the necessity not only of comprehensive awareness training but also of building a security culture that extends to all members of the organization.

Addressing the human element in cybersecurity requires an approach that combines technical defenses with continuous education, cultural adaptation, and psychological awareness. Organizations must create an environment where employees feel empowered to question unusual requests, verify sources of communication, and report potential incidents without fear of blame.

3. Pretexting is a social engineering technique where an attacker fabricates a scenario to manipulate individuals into divulging confidential information.

How To Strenghten the Cybersecurity Chain

As technical defenses become stronger, the main challenge in cybersecurity increasingly centers on human behavior. While technology helps reduce risk, resilience depends on developing a strong security culture that shapes how people think and act in relation to security in their daily work. Security awareness and culture should not be treated as a compliance exercise but as an ongoing educational process that equips employees with the skills to recognize and respond appropriately to manipulative tactics.

A healthy security culture addresses this by openly valuing and even rewarding the act of reporting, regardless of the outcome.



The European Union Agency for Cybersecurity (ENISA) uses seven key dimensions to approach security culture:

1. **Attitudes**
   How employees feel about security and their relevance to their work.

2. **Behaviors**
   The visible actions employees take to protect systems and information.

3. **Cognition**
   The understanding of threats, risks, and protective measures.

4. **Communication**
   How effectively security messages, feedback, and incidents are shared across the organization.

5. **Compliance**
   How well-established rules, guidelines, and procedures are followed.

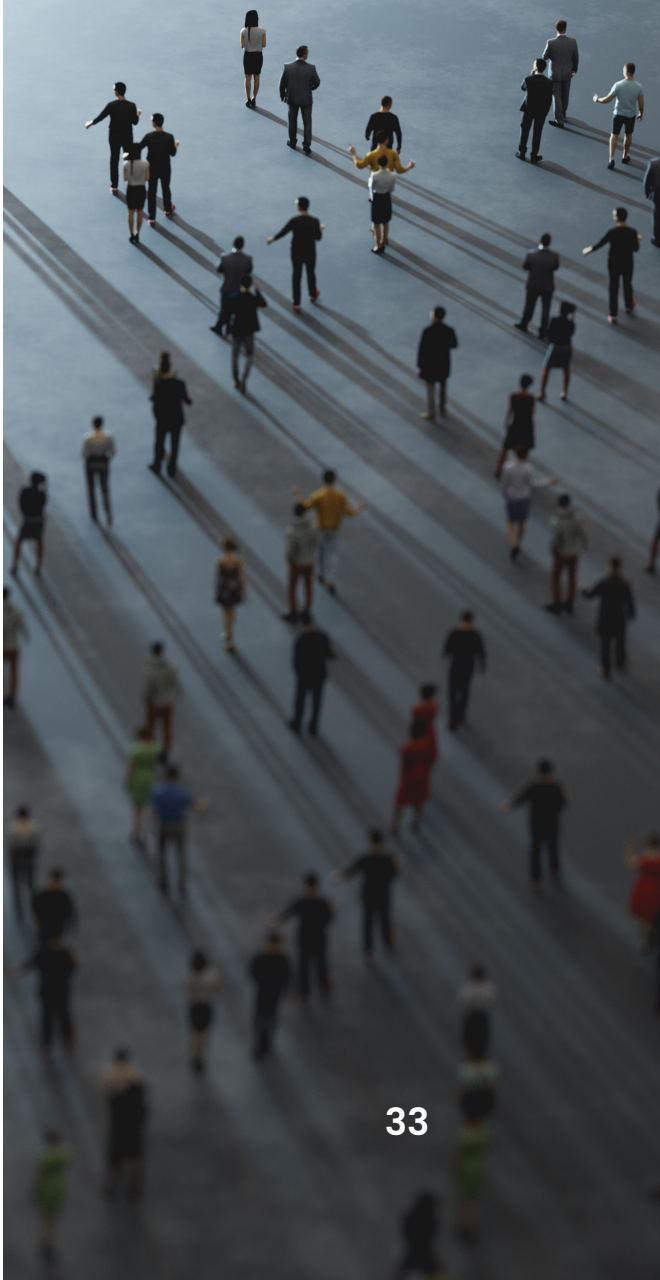
6. **Norms**
   The informal expectations within teams that influence what is seen as acceptable or careless security behavior.

7. **Responsibilities**
   The clarity with which employees understand their individual and collective roles in safeguarding information.

A robust security culture reflects the shared values, attitudes, and habits that influence how individuals handle information, respond to unusual requests, and make decisions when under pressure. When employees view security as part of their professional responsibility, rather than a technical requirement, they become an active line of defense against manipulation and error.

Leadership commitment is another decisive factor. Visible leadership support shows that security is not only an IT issue but a shared organizational value that contributes to trust, integrity, and operational stability. Developing a mature security culture is an ongoing process that requires consistent, deliberate effort and evolves alongside the threat landscape.

By aligning technology with cultural and behavioral change, organizations can reduce human vulnerabilities, improve detection and response, and make secure behavior the natural and expected way of working.



Threats from Within

"It's Coming from Inside the House"

Truesec was called in to assist with a serious IT incident. The victim, a medium-sized enterprise, had received no warning when parts of its IT environment suddenly stopped responding. No encrypted files, ransom note, or any other clue as to what had happened or who was behind it.

Initially, Truesec treated this as a potential active external threat. It was apparent someone had purposefully disabled functions and deleted critical data. However, as the investigation progressed, forensic analysis revealed facts that seemed inconsistent with this assumption.

The available logs indicated that the threat actor's activity originated from an IP address identified as a Tor (The Onion Router) exit node.

There was, however, no indication of which account was used at the time. The threat actor also appeared to possess detailed knowledge of both the infrastructure and its security controls. Leveraging this insight, they disabled key security features within the cloud infrastructure platform.

With defenses neutralized, they carried out destructive actions, including the complete deletion of critical resources and systems, causing severe operational disruption. After disabling security features and deleting resources, systems, and data, the threat actor proceeded to target backups, snapshots, and other copies of the systems. These were also erased, significantly limiting recovery options and maximizing impact.

The threat actor then shifted focus from the cloud to the on-premises environment, targeting central infrastructure components, networking equipment, and storage solutions with a series of destructive actions. Several of these succeeded, causing significant impact, whereas others failed due to insufficient permissions.

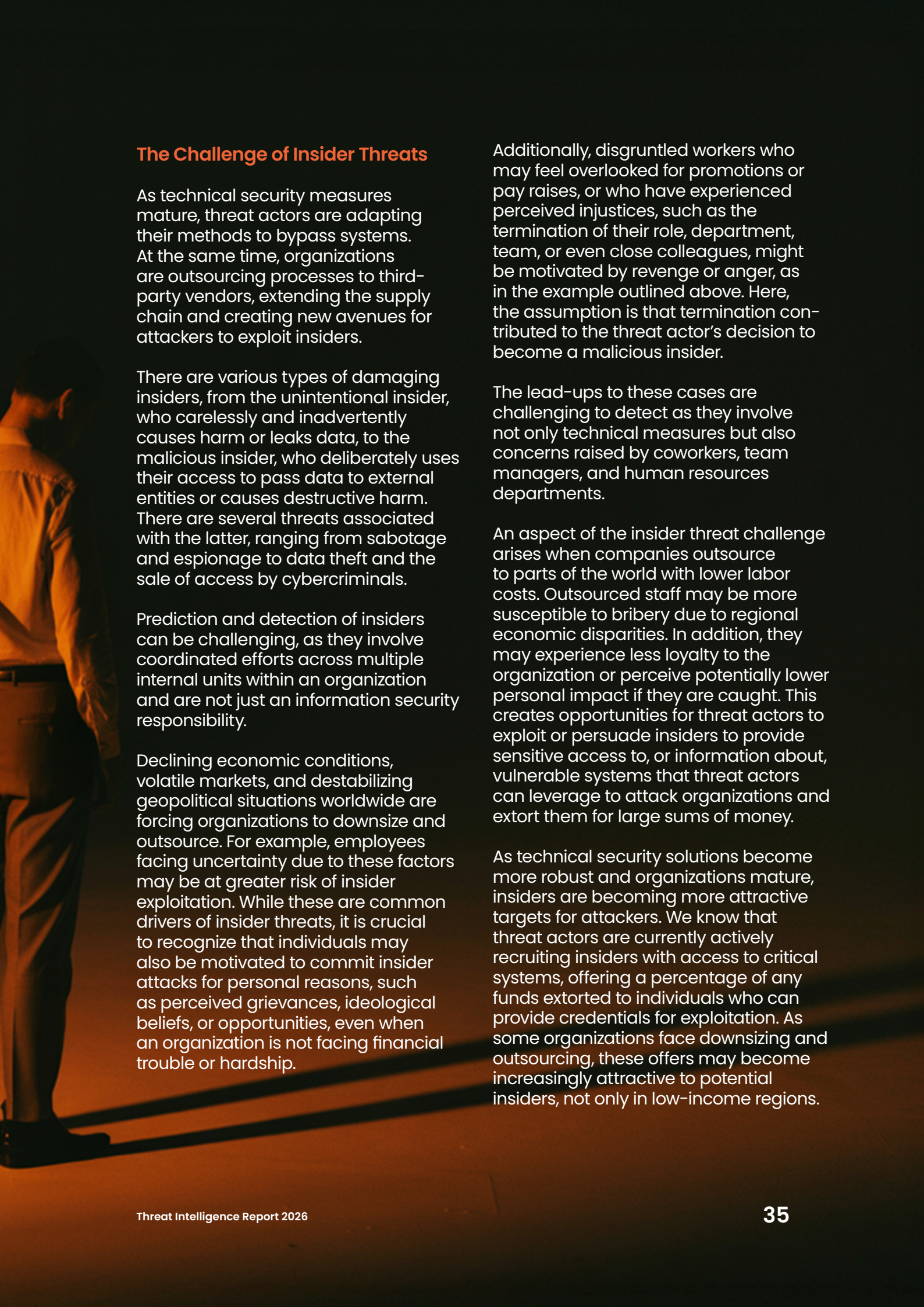
Even after the investigation had begun, the attacks continued. This time, the methods changed from manual interactive actions to a more automated, script-based approach. This enabled the execution of destructive commands at scale, effectively wiping out numerous systems, resources, and datasets.

Given the context, it may not be surprising to learn that the threat actor was in fact a disgruntled employee, just days away from leaving the company. This individual attempted to conceal the sabotage by using anonymization services, shared accounts, and various other obfuscation methods.

Fortunately, these efforts were not enough to erase all traces. Forensic analysis ultimately revealed the perpetrator's identity, allowing intervention to halt further damage.

So why did this person do this? Ending their employment likely played a significant role, but pinpointing why some individuals choose to act this way remains challenging. However, many possible answers will be outlined in subsequent parts of this section.





The Challenge of Insider Threats

As technical security measures mature, threat actors are adapting their methods to bypass systems. At the same time, organizations are outsourcing processes to third-party vendors, extending the supply chain and creating new avenues for attackers to exploit insiders.

There are various types of damaging insiders, from the unintentional insider, who carelessly and inadvertently causes harm or leaks data, to the malicious insider, who deliberately uses their access to pass data to external entities or causes destructive harm. There are several threats associated with the latter, ranging from sabotage and espionage to data theft and the sale of access by cybercriminals.

Prediction and detection of insiders can be challenging, as they involve coordinated efforts across multiple internal units within an organization and are not just an information security responsibility.

Declining economic conditions, volatile markets, and destabilizing geopolitical situations worldwide are forcing organizations to downsize and outsource. For example, employees facing uncertainty due to these factors may be at greater risk of insider exploitation. While these are common drivers of insider threats, it is crucial to recognize that individuals may also be motivated to commit insider attacks for personal reasons, such as perceived grievances, ideological beliefs, or opportunities, even when an organization is not facing financial trouble or hardship.

Additionally, disgruntled workers who may feel overlooked for promotions or pay raises, or who have experienced perceived injustices, such as the termination of their role, department, team, or even close colleagues, might be motivated by revenge or anger, as in the example outlined above. Here, the assumption is that termination contributed to the threat actor's decision to become a malicious insider.

The lead-ups to these cases are challenging to detect as they involve not only technical measures but also concerns raised by coworkers, team managers, and human resources departments.

An aspect of the insider threat challenge arises when companies outsource to parts of the world with lower labor costs. Outsourced staff may be more susceptible to bribery due to regional economic disparities. In addition, they may experience less loyalty to the organization or perceive potentially lower personal impact if they are caught. This creates opportunities for threat actors to exploit or persuade insiders to provide sensitive access to, or information about, vulnerable systems that threat actors can leverage to attack organizations and extort them for large sums of money.

As technical security solutions become more robust and organizations mature, insiders are becoming more attractive targets for attackers. We know that threat actors are currently actively recruiting insiders with access to critical systems, offering a percentage of any funds extorted to individuals who can provide credentials for exploitation. As some organizations face downsizing and outsourcing, these offers may become increasingly attractive to potential insiders, not only in low-income regions.

Mitigating Insider Threats

Although the challenge posed by insider threats may seem intangible, there are ways to protect against them. Organizations need to carefully assess their employees, understand the risks of outsourcing critical IT functions, and ensure that third-party providers adhere to robust security standards.

It is essential to recognize that the definition of "insider" extends beyond direct employees to include external entities such as contractors, outsourced staff, and third-party service providers, who may also have privileged access and therefore pose similar threats to organizational security. Employees with access to sensitive data or critical systems should be thoroughly and continually vetted to monitor for any risk factors that may indicate potential exploitation, ideally through stringent due diligence processes and continuous security vetting. Prior involvement in criminal activity, financial strain, or unethical behavior should raise concerns and indicate a potential for insider threats, prompting actions to either investigate or contain.

Because insider threats can manifest in complex ways, it is essential to take a diverse approach to preventing and mitigating them. An effective defense should consider both the policy level, the human aspect, and technical controls.

At the policy level, insider threats should be recognized and incorporated into risk governance measures. Regular educational awareness for all employees and staff on the risks posed by insiders, along with training in secure practices and reporting suspicious behavior, is crucial. This will foster a security-conscious culture in which employees understand their role in protecting sensitive information and in which security is everyone's responsibility.

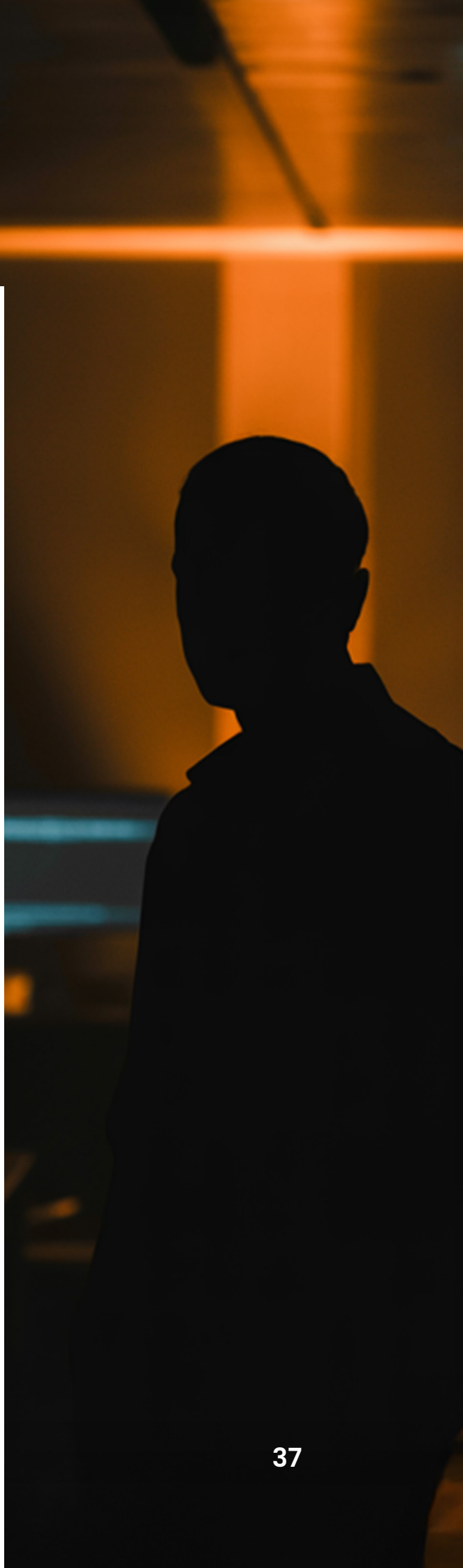
However, it is equally vital that these measures are implemented thoughtfully and respectfully. Encouraging vigilance should never result in a culture of suspicion or "witch hunts" against colleagues. Employees must be educated not only to recognize and report risks but also to understand the importance of fairness, confidentiality, and the avoidance of unfounded accusations.

Proper handling helps maintain trust, respect, and a positive working environment, ensuring that security measures protect both the organization and its people.

The human aspect is critical, particularly given the shift toward social engineering in today's threat landscape. Furthermore, Truesec data indicates that more than half of all detected insider incidents are initiated by colleagues who raise concerns about a coworker. This highlights the importance of the human element in insider threat prevention.

Implementing technical controls is indispensable for preventing insider threats. Today, human and digital behaviors are deeply intertwined and cannot be effectively addressed in isolation. A robust approach to mitigating insider threats should therefore also rely heavily on robust security technologies that continuously monitor assets to detect and prevent unwanted access or unauthorized behavior.

Downloads of large amounts of data or access at odd hours should be logged and investigated. Employees who attempt to elevate privileges or access resources or data beyond their assigned role should raise concerns. Clear incident response procedures should be in place for suspected insider threats, where collaboration across departments is planned and trained to identify and respond quickly and efficiently.



When the Threat Doesn't Go Away

The Eternal Victim

In 2025, Truesec responded to a severe ransomware attack.

One of the first steps was to conduct a forensic investigation to determine whether any data could be recovered, identify how the threat actor gained access, and determine an appropriate course of action for recovery and restoration.

The forensic analysis indicated that the threat actor likely had gained access through compromised VPN credentials. However, additional anomalies were detected. The investigation identified artifacts from what appeared to be older incidents. Eventually, it reached a point at which files were found that had been encrypted by a different encryptor, belonging to a completely different ransomware actor.

As the forensic analysis continued, the traces continued to point further and further back in time, seemingly to no end. Eventually, it reached a point at which files were found that had been encrypted by a third encryptor, and by a completely different ransomware actor than in the previous two cases. At this stage, the question had to be asked: What had really happened here? Why do traces of at least three different encryptors, each linked to separate ransomware groups, appear within a few months of each other?

The question was referred to the victim organization, which reluctantly reported that this was the fifth time it had been encrypted this year alone, and that each time, its service provider had responded by simply restoring the environment from backups to a state before encryption.

The service provider had not considered that their restoration would not fix the vulnerability that had let the first ransomware actor in, which was presumably still open to new threat actors. Each successive ransomware attack also meant that a new data dump from the network had been stolen, likely containing additional information that could be used to compromise them again.

Further analysis revealed that some of these attacks may have been carried out by the same threat actor, who used different brands in separate attacks, possibly a RaaS affiliate using different brands in multiple attacks. Other artifacts clearly belonged to different groups altogether, using different methods to take over the environment.

Once attackers know how to breach your environment, they can exploit that weakness repeatedly unless you take proactive steps to ensure you understand how to prevent future incidents.



The Challenging Cycle of Re-Victimization

A cyberattack rarely ends with the ransom note or the restoration of encrypted files. While the victim organization scrambles to contain the damage, communicate with stakeholders, and meet immediate regulatory deadlines, the cybercriminal is already busy trying to monetize the breach further.

Regardless of whether the victim pays the ransom, cyber extortion groups will attempt to remonetize the stolen data; every log file, configuration setting, temporary cache, browser history, saved credential, session cookie, autofill entry, and even browser extension data. This is not opportunistic theft; it is deliberate information gathering.

Consider a single user's browser profile. Browsers such as Chrome, Edge, or Firefox store far more than browsing history. They retain saved passwords (often weakly encrypted with OS-level keys), autofill data (names, addresses, payment details), session cookies (allowing instant re-authentication to cloud services), and OAuth tokens (granting persistent access to SaaS platforms). A mid-level manager's local profile might contain 50+ credentials: internal VPN portals, AWS consoles, Slack workspaces, GitHub repositories, and even personal accounts used for work-related tasks.

These are sometimes overlooked when applying enterprise policies such as multi-factor authentication (MFA). Once exfiltrated, attackers can crack them offline using readily available tools, chain them with other stolen data, and impersonate legitimate users months later, long after the initial incident has faded from the headlines.

This data-hoarding behavior represents a strategic evolution in cybercrime. Stolen data from a breach can be remonetized by leveraging it in new extortion schemes, breaches, or cyber fraud. Data lost in a single breach can fuel future cyberattacks.

During the reconnaissance phase of an intrusion, attackers methodically build a living map of the victim's digital and, more commonly, human ecosystem. They catalog the IT environment, including Active Directory structures, firewall rules, VPN configurations, and cloud tenancy details. They trace network architecture, documenting internal IP ranges, subnet layouts, jump hosts, and lateral movement pathways.

Information gathered during reconnaissance may also persist after a failed cyberattack. Scavenger criminals will harvest data from failed extortion attempts and repost them as new attacks, further damaging the victim's brand.

Log sellers are a relatively new type of cybercriminal that often represent the final stage in the life cycle of a data breach. Log sellers hoard stolen data from hundreds of successful and failed data extortion attempts. They structure and enrich data in databases, then profit by selling access to criminals who can exploit it for purposes ranging from launching ransomware attacks to committing fraud and scams. Even state-sponsored actors purchase intelligence from these log sellers.

Attackers may also view victims who have been successfully attacked before as easy targets for future attacks, since they may not have had time or resources to fully recover or update their security.

Stolen data from previous attacks, obtained from log sellers, can give attackers a significant advantage. They can gain intimate knowledge of the target environment. A forgotten service account found in a stolen config file can easily become the next entry vector. Phishing emails now reference real internal project codenames, upcoming board meetings, or personal details lifted from browser history. A stolen session cookie can grant temporary admin access before MFA reasserts. Even a single dormant credential, such as a VPN account with SMS-based MFA that rotates infrequently, can be reactivated.



From Victim to Resilient Target

How do you protect yourself from someone who has stolen your data and is now using it to ransom you, attack you again, or sell it to the highest bidder? There is no perfect solution, but there are many things you can do.

At its core, data is what threat actors primarily seek, regardless of its form. That means you can work with various data-handling methods. Avoid collecting and storing data that you do not need. Archive or delete anything that has lost its value, necessity, or importance to you; it may still be highly sensitive and valuable to someone else.

Understanding where your data resides, what is sensitive, who and what can access it, and how you know when unauthorized access has occurred, also remains crucial. Furthermore, modern data classification tools strike a good balance between security and usability, making them highly viable options for further protection of your data.

Ideally, you want to design your infrastructure with data sensitivity in mind, so that the most sensitive data is protected not just by a single software application, but by layered security features across multiple levels.

Many of these suggested solutions can be challenging to implement because they often affect the entire organization. However, it is possible to do this in steps: start with the simpler variants, protect the most sensitive data, and then expand from there.

But what can you do when the unfortunate happens? When data has been stolen or has inadvertently ended up in the wrong hands. Here is where it gets difficult, as there is no perfect solution.

> There is ample evidence that paying criminals' ransom demands does not guarantee your troubles are over or that your data is safe. Criminals will always find new ways to monetize your stolen data. However, there are some steps you can take to limit the impact.

> Evaluate your monitoring capabilities of the dark web as well as public sources. If your data is out there, accessible or readable, you at the very least want to know where and what. This allows you to better assess the damage, risk, or potential threats its exposure may pose.

When data resides in a location or platform of relevant legitimacy or reputability, a takedown request may be possible. Some platforms offer removal or other measures when stolen data is published or shared through their solutions.

Reporting to authorities can sometimes lead to actions being taken that may better protect your organization.

Assume Breach is not a new strategy, and the goal today is not to prevent every single breach, because that is virtually impossible. Instead, ensure that even when the attacker holds the blueprint, your house remains unlivable for them.

By assuming compromise, eliminating trust, and building intelligence-aware defenses, organizations have a better chance of breaking the cycle of re-victimization.





The Complexity of Large and Multinational Organizations

The Chain Is Never Stronger Than the Weakest Link

Throughout the year, Truesec has handled several incidents in which threat actors have followed patterns like those described in this section; however, the following example is an amalgamation of several actual incidents.

A ransomware attack hit a European enterprise with an international presence. The corporate IT was fully encrypted, the business was at a standstill, and money was bleeding out.

During the forensic investigation of the incident, Truesec discovered that the threat actor established a foothold via a firewall serving a subsidiary in Asia. The local IT admins reported that MFA was too slow in the remote area, so they enabled local accounts on the firewall without MFA to circumvent the problem. As these accounts were intended only for short-term troubleshooting, they had generic names and default passwords. This enabled the threat actor to immediately guess the valid credentials, which were the default credentials for the specific firewall, and in turn, access the environment.

This gave the threat actor an initial foothold in the environment, enabling them to execute tools from their own machines via the VPN solution and target systems

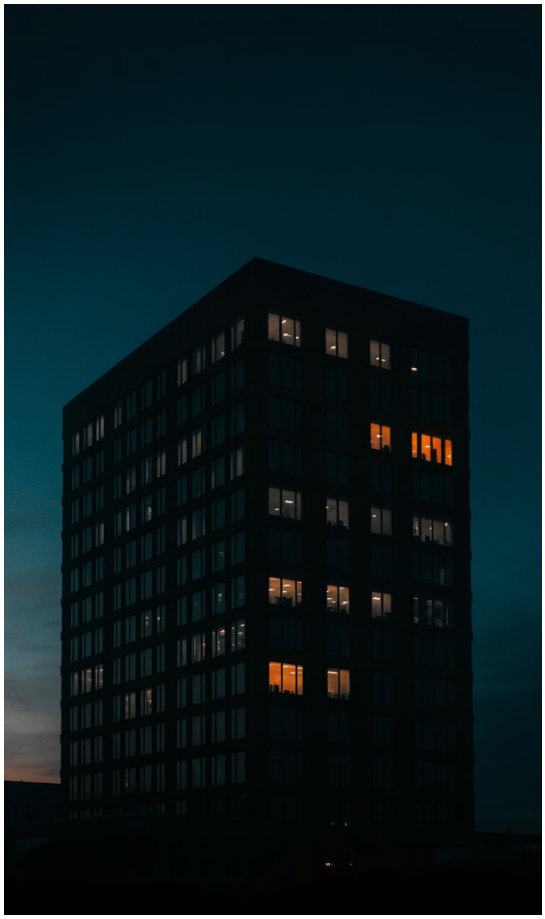
within the IT environment. They began scanning the environment to understand what was present, using a combination of network scans and Domain Name System (DNS) requests. The DNS requests were used to identify the Microsoft Active Directory domain controllers. The network scans revealed which systems had a remote management port and, in some cases, were accepting credentials obtained by the threat actor.

After this initial discovery and reconnaissance, the threat actor transferred a vulnerable driver to one machine that they could access. This driver exhibited behavior that could enable the remote extraction of Microsoft Windows registry files. However, when the threat actor attempted to execute it, the installed EDR agent detected and blocked the activity. Upon realizing that their initial attempts had failed, the threat actor disconnected the VPN session to avoid further detection.

Around 24 hours later, the threat actor reconnected by starting a new VPN session. They conducted lateral movement from the VPN to a server via Remote Desktop Protocol (RDP). The threat actor then obtained additional credentials from other users who had visited the servers. Shortly after, the threat actor moved to another server, again using RDP.

Throughout the period leading up to that point, the threat actor did not download any hacking tools on the victim's machine. Instead, the threat actor ran the hacking tools on their own machine through the VPN connection.

This second server was part of a Microsoft Hyper-V cluster that hosted virtual machines serving the entire global business. In quick succession, the threat actor copied malware files from the VPN to the Hyper-V server. From there, they copied the same file to all the virtual machines in the cluster and executed it on them. This malware file was the encryptor that rendered the data on all virtual machines completely unreadable, bringing the entire IT environment to a grinding halt. This was also the first time the threat actor had introduced malware onto the compromised environment, aside from the initial failed attempt with the vulnerable driver.



The Challenge That Comes With a Global Presence

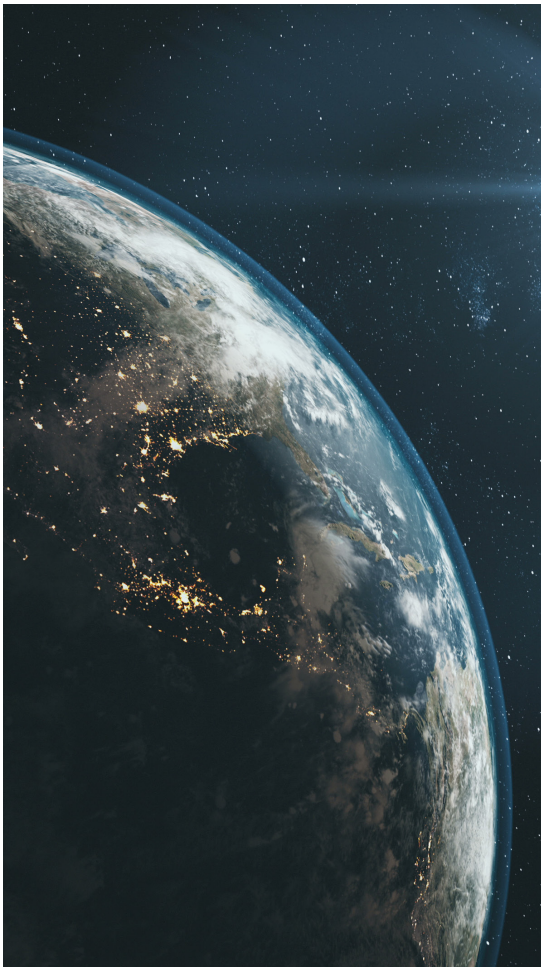
In our modern globalized world, companies have offices and teams working across the globe, all connected through their corporate network. VPN solutions and interactive log on capabilities, such as RDP, help employees feel like they can access everything seamlessly, no matter where they are in the world.

In a typical open corporate network, adversaries need only to find one vulnerability, one misconfigured server, one careless employee, or one unpatched system in one single office anywhere in the sprawling global network. At the same time, defenders must maintain flawless protection everywhere, at all times, across every culture, every jurisdiction, and every time zone.

It's not necessarily fair, but the reality of cybersecurity in the multinational enterprise is complex. The attack surface expands when the network spans the world. Vital IT operations may be outsourced to regions chosen for low labor costs rather than good security practices. Global supply chains may require a presence in high-risk countries where government surveillance is endemic.

Company culture is one thing when you are in the same office as the CEO in Europe, but it is something entirely different when you're in a back office in Asia, working for minimum wage, not really knowing the board, the brand, or the company history, in a country you've never visited.

Maintaining cybersecurity and protecting valuable intellectual property in a global enterprise requires careful network segmentation, with roles and privileges assigned as securely as possible so that a breach at a weak point doesn't compromise the entire environment.



Using Technical Controls To Prevent Global Attacks

When large multinational organizations have their entire global environment compromised, the primary reason the threat actor can move throughout the network is a lack of proper network segmentation: once connected, the threat actor has access to the entire internal network. More often than not, organizations provide network access when a lower level of access would suffice. For example, information/data access or application access. This can be achieved without granting the person network access by using solutions such as cloud storage (e.g., Microsoft OneDrive or application gateways).

It is neither necessary nor advisable to allow access to all assets once a user is logged in. Users need access only to the systems relevant to their tasks, usually only a handful of the hundreds of systems available to the organization. Connecting to a server via RDP from a VPN or from any user workstation is often unnecessary. Instead, a user's daily access typically requires only a few services, such as Kerberos or SMB.

Proper network segmentation enforces access based on necessity. Karen from Accounting needs access to her finance and business applications, not to the management ports of the servers themselves. Similarly, John from reception at the Sweden office only needs access to the local access control system, not to the RDP port on the file server in the U.S. office.

If segregation is not in place, a threat actor can move from a server to an infrastructure server. The infrastructure servers, core networks, and storage networks constitute the "fabric" on which the whole organization's IT systems are built and operate. As such, this is the most critical component of the organization's technologies. If a threat actor gains access to this fabric, the potential for catastrophic damage is high.

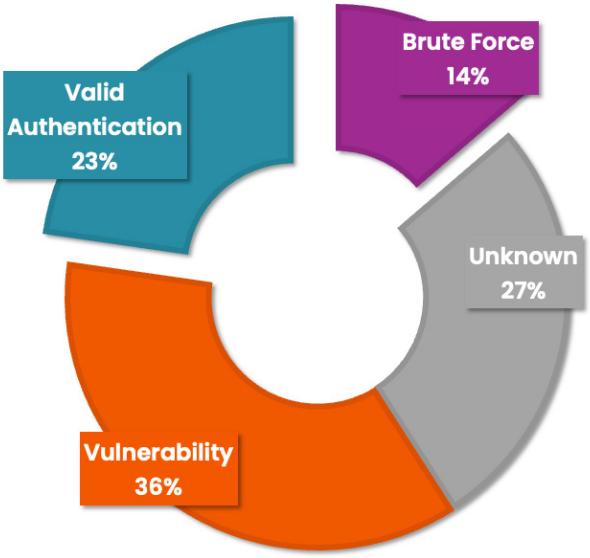
Truesec recommends using tiering[4] to enforce proper segregation, and the most logical place to start is the fabric. From a network standpoint, this means refusing all connections to any management port of the fabric systems except for dedicated privileged access workstations (PAW)[5].

4. Read more: www.truesec.com/security/active-directory-tiering

5. A Privileged Access Workstation (PAW) is a hardened, dedicated computer, physical or virtual, used exclusively for performing administrative tasks on critical systems. It's a key security control designed to protect high-value accounts and systems from compromise.

Password Attacks Are Still Relevant

More than a third of the ransomware incidents handled by Truesec in 2025 began with attackers using valid usernames and passwords to access exposed VPN gateways or terminal servers.



The Challenge of Preventing Attackers from Logging In

Almost 14 percent of valid credentials used in ransomware attacks handled by Truesec CSIRT in 2025 were obtained through password spraying. For the rest, it's largely unknown how the credentials were compromised. While phishing remains a well-known method for stealing credentials, it is far from the only one. There is a great deal of information-stealing malware available for purchase on criminal dark websites. Previous data breaches can also lead to credential leaks. The explosion of online services that use credentials for login, combined with frequent data breaches, has provided threat actors with vast lists, called dumps, of potential usernames and, sometimes, passwords to leverage against organizations.

Often, the usernames in these dumps are email addresses linked to specific companies, making the potential victims easy to target.

The passwords in these dumps may be either in plain text or hashed. In the former case, they are available in clear text and can be immediately exploited. Even when passwords are stored in a hashed form, they can still be cracked, leaving attackers with the actual credentials to log in.

Truesec has observed several different methods used to gain valid credentials.

One type of attack exploits password reuse across multiple platforms. With the explosion of online services mentioned above, this is highly relevant. Imagine an employee who uses the same password for both a cloud service and the company's VPN. If the cloud service suffers a data breach and user credentials are leaked, a threat actor can obtain that data, identify the employee's email and password, and simply try those same credentials on the corporate VPN. If they work, the attacker gains access, and voilà, classic credential stuffing in action.

A step beyond password reuse is when threat actors do not have the exact password for an account but instead possess lists of potential usernames and passwords. This enables the notorious password-spraying attack, in which attackers systematically test these combinations against exposed systems, in the hope of finding a match. This is especially effective against organizations that set a default password at either account creation or when a password reset is requested.

Large botnets available for hire on the darknet are commonly used for DDoS attacks but also for large, distributed password-spraying attacks. By distributing password-spraying attempts against hundreds of accounts among tens of thousands of bots, it's easier to avoid triggering warnings.

If a password-spraying attempt fails or no password list is available, threat actors will generate their own list of password candidates. This list can be quite extensive, often containing the name of the company and variations, and the list of the top 10 most used passwords in 2025[6] and even the list of the top 500 worst passwords[7]. Truesec responded to an incident in 2025 in which the threat actor tried more than 10,000 combinations of usernames and passwords before finding a valid pair.



6. Read More: www.passwordmanager.com/most-common-passwords-latest-statistics

7. Read More: weakpass.com/wordlists/500_worst_passwords.txt

A Multi-Pronged Approach of Prevention, Detection, & Response

When it comes to defending against password attacks, MFA remains the most effective countermeasure. The concept of MFA is straightforward. In addition to a password, the account has one or more additional forms of verification. These factors are what you have, what you know, and what you are. It can include a client certificate, a token generating one-time passwords, or an application that requires manual approval, to name a few. Often, authentication relies on a password and one additional factor, so-called two-factor authentication (2FA), but nothing prevents the use of more than two factors.

In an MFA scenario, a threat actor with a valid username and password is hindered by the remaining additional factor. Note that our use of "hinder" and not "prevent" is intentional. MFA is not bulletproof, and it comes with its own challenges.

To begin with, deploying MFA organization-wide is difficult because MFA solutions that cover all network assets are rare. In addition, it is unfortunately common to use less effective MFA methods. For example, SMS-based MFA is considered one of the least secure options due to its vulnerability to various attacks that may expose the one-time code to threat actors.

When it comes to resilience, MFA methods that use separate hardware storage are much more resistant to attacks. Also, MFA techniques based on public key infrastructure (PKI) or FIDO2 are very robust against sophisticated phishing attacks due to their cryptographic binding[8].

MFA protects against password attacks, but threat actors are creative and have found ways to bypass MFA. Two standard techniques used are MFA fatigue and the Adversary-in-the-Middle (AiTM) technique. MFA fatigue leverages push notifications. The threat actor, knowing the correct password for an account, submits hundreds of requests to the system, which results in an equal number of approval requests sent to the user. The attack succeeds because the victim usually gets tired of the flood of incoming requests and accepts it just to end the annoyance. In AiTM, the threat actor is intercepting the user's login session by using a proxy server to position themselves between the user and the legitimate login page, stealing the credentials and the one-time MFA code.

Threat actors may also call the help desk and use social engineering to request a password reset while deactivating MFA. They then usually call the help desk, posing as an employee with a lost or stolen phone, who lacks MFA access and

8. *Microsoft Word - IAM Group 2 MFA SSO Challenges FINAL*



needs help regaining control of their account. Threat actors who conduct these types of social engineering attacks are usually highly skilled, have done their homework on the target company and its employees, and are therefore highly convincing, making them extremely difficult to detect for untrained individuals.[9] This is not a technical attack; it falls under social engineering, which we cover in our chapter, "The Constant Evolution of Social Engineering."

Knowing what the threat actors know helps you act on what matters. In the age of infostealers and ongoing data breaches, it is essential to identify leaked credentials quickly. An effective way to do this is to use a service that scans the dark web for leaked credentials. Such services can provide alerts whenever leaked credentials matching their domains are discovered, which enables preventive actions such as resetting passwords, implementing additional monitoring, or imposing restrictions, for example, Conditional Access, on affected accounts. Quick interventions are vital in these scenarios, as a threat actor who has logged in with valid credentials can be extremely difficult to detect.

While prevention and proactivity go a long way, there will always be that one time when, despite all measures taken, the threat actor can get in, and when it comes to security, "just one time" can be enough to sink a company.[10] It is thus paramount to detect the signs of a potential attack, whether successful or not, early enough, and with as many details as possible to enable a timely, adequate response. Monitoring login failures, their sources, and subsequent successful authentications often yields valuable insights into adversaries attempting to gain network access.

There, it pays to be discerning in the observations. Authentication attempts against well-known or generic account names are now almost inevitable and often just background noise[11]. However, as soon as the attempted authentication matches a valid username in the organization, an alert must be triggered.

As the adage goes, "detection without response is meaningless". Readiness and response playbooks make a huge difference. Whether it is the help desk, IT, or the SOC, teams must be equipped to reset multiple passwords swiftly, block compromised users from authenticating externally, and revoke access to cloud platforms instantly. Preparing and rehearsing these measures will make all the difference when every second counts.

9. Scattered Spider | CISA
10. Ransomware: from incident to bankruptcy - PONT Data&Privacy
11. This is also a good reason to not to leave default accounts on exposed systems.

Malicious Packages Pose Software Supply Chain Risk

Throughout the year, we have seen a range of breaches targeting the development chain or parts thereof. In late August 2025, reports emerged of malicious versions of several Nx packages being published to npm, the world's largest software registry. This campaign, dubbed S1ingularity, involved code designed to exfiltrate sensitive data such as credentials and crypto wallets and upload it to attacker-controlled GitHub repositories.

Shortly thereafter, a second major incident, referred to as "Shai-Hulud", compromised more than 500 npm packages. The malicious code once again focused on several types of credential theft but also included worm-like behavior, spreading rapidly by injecting malicious code into additional packages and publishing compromised versions to registries.

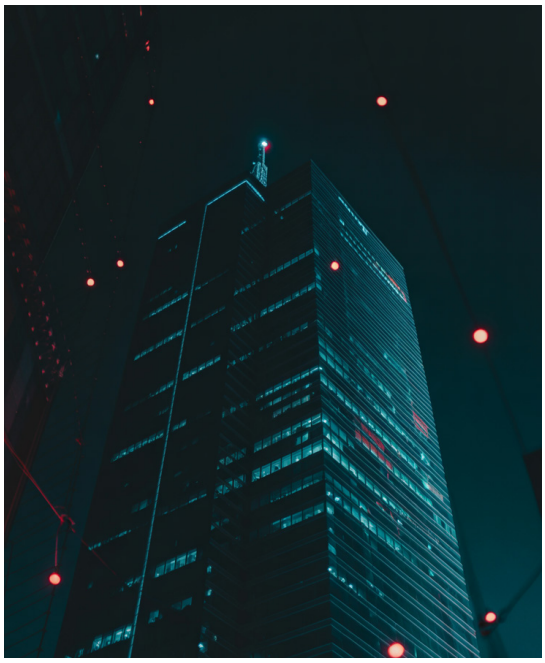
In October, we saw a different, albeit similar type of supply chain attack. The Open VSX registry, which serves extensions for Visual Studio Code, was targeted by Glassworm, a self-propagating VSCode extension worm. Several Open VSX extensions were compromised to include code that aimed to steal credentials, drain cryptocurrency wallets, and even establish command-and-control (C2) channels. Later, malicious extensions in the official Visual Studio Code repository were found. Like "Shai-Hulud", this campaign incorporated self-propagating mechanisms that enabled automated spread across the ecosystem.

While we have seen these types of breaches for several years, they have transitioned from a specific type of focus, commonly crypto wallets, to a broader and more impactful approach. Threat actors now commonly deploy various types of information stealers and similar malicious code, which can significantly impact both individuals and the organizations they belong to.

The fundamental risk in these attacks stems from the profile of impacted users and devices. Those most likely to download and integrate third-party packages are typically highly privileged users, such as developers or system administrators, often possessing broad access across organizational environments. These accounts typically operate with elevated permissions and store sensitive assets, including API keys, SSH credentials, and access tokens, on their local systems.

When such accounts are compromised, the supply chain effect intensifies, as stolen credentials can enable lateral movement into critical infrastructure components, such as deployment pipelines, CI/CD servers, and source code repositories. This creates a cascading impact, allowing attackers to infiltrate multiple layers of the ecosystem and potentially compromise entire development environments. Notably, malicious

packages may reach CI/CD servers directly if, for example, they are used in the build process. If that happens, other types of credentials that may not be present on developer devices could be compromised if used as part of the build process.



Both open source and closed-source software face similar security challenges, but the underlying dynamics differ. Open source projects often lack dedicated security budgets and resources, leaving critical packages and widely used repositories without formal requirements or rigorous security vetting. This raises questions about how vulnerabilities are addressed and security measures implemented when funding and focus are limited.

Conversely, open source code benefits from community-driven scrutiny, which can sometimes exceed what an in-house team for a closed-source project might achieve. However, this advantage is inconsistent and depends heavily on contributor engagement and expertise.

Closed-source software is not immune to these issues, but organizations typically enforce structured review processes, including procurement checks, security assessments (often rudimentary and secondary priorities), and testing phases before deployment. In contrast, open source components are often downloaded and executed within minutes of discovery, significantly increasing the risk of introducing unverified code into production environments. The boundaries between open and closed-source software can also be blurred, as many closed-source projects depend on open source components.

The widespread lack of maturity in secure development practices remains a critical issue. When this is combined with the absence of structured processes for managing third-party software and the use of highly privileged devices, the risk profile escalates dramatically. Conditions like this create an environment where vulnerabilities, malware, or generally insecure components can propagate unchecked, and compromise can lead to deep, systemic breaches across development and production ecosystems.



Revisiting Core Security Concepts in a World of Rapid Development

Software developers are now a significant target for threat actors. There is no single, simple solution to reduce these threats. It is essential to revisit foundational security principles such as least privilege and administrative isolation.

The combination of local administrative privileges and access to various build solutions, git repositories, cloud environments, CI/CD pipelines, APIs, and even infrastructure directly in a DevOps environment creates a broad attack surface.

Ideally, the area where developers build and test new software solutions should be separated from the production environment, so that only safe, vetted code is introduced into a production environment with separation at the AD level. Reality, of course, is far more complex, and this concept would only address some of the issues.

Even with careful separation between development, test, and production builds, each build typically contains code packages that, in turn, include many dependencies, often patched at varying frequencies. Each patch may introduce malicious updates or inadvertent vulnerabilities in the carefully vetted production build.

This is where asset management comes into place. Expanding this to the software development lifecycle, regularly reviewing which packages are used, and removing those that are no longer needed is crucial for maintaining a clear inventory of dependencies across your codebase.

You need to continuously identify risks, monitor for vulnerabilities, find deprecated packages, and notice unauthorized changes across your codebase. In most cases, effective tooling or processes to support this are also needed.

Despite our best efforts, malicious code can still be introduced. Some vulnerabilities only become apparent after exploitation. Protecting your software pipelines, much like defending against zero-day vulnerabilities, is challenging at best.

Having comprehensive asset management that can identify not only the affected package but also the exact version, download timestamp, and whether it was executed will also significantly reduce the time it takes to identify and respond if some part of the code has been compromised.

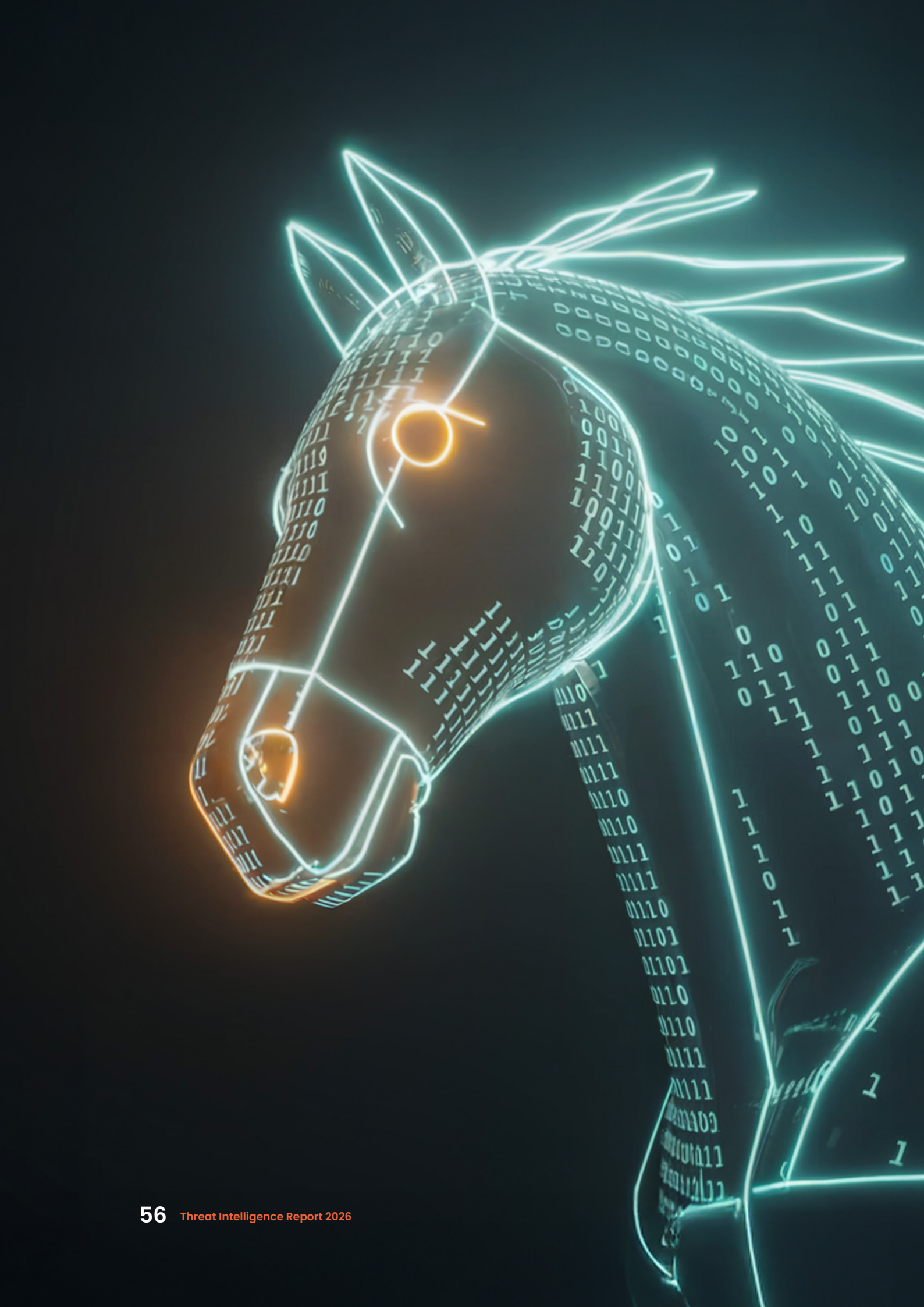
One key factor in minimizing the risk of introducing malicious code into projects is to delay immediate adoption of newly released packages. While this approach may seem counterintuitive, given the common practice of rapid updates to patch security flaws, it can be prudent in environments where new releases have not undergone stringent security vetting.

Allowing a short delay gives the community or vendors time to identify and remediate potential vulnerabilities before deployment, reducing the likelihood of introducing compromised code into production. There are, of course, exceptions when a particularly severe known vulnerability is actively exploited by attackers, even if the patch is intended to address it.

Minimizing the impact of supply chain breaches requires a layered approach that addresses vulnerabilities before they are exploited and ensures rapid containment when incidents occur. General advice on securing your environment, including detection and response capabilities, applies here in particular. An EDR agent generally will not detect flaws in a malicious code package unless it is already known to be bad, but it can react during execution if it introduces a backdoor or conducts other malicious activity.

For more detailed help in securing your software supply chain, please visit the Truesec blog post by scanning the QR code.

Npm Supply chain Attacks: How to Reduce Risk



Deep Dive:
The Malicious PDF Editor



In June 2025, a series of Google Ads campaigns began promoting the PDF Editor by AppSuite. Truesec has identified at least five distinct Google campaign IDs, suggesting a widespread campaign primarily targeting Europe. The ads pointed to several websites that appeared to be AI-generated and hosted the PDF editor. The PDF Editor file was heavily obfuscated, and many independent researchers agreed that the malicious code appeared to be generated by AI/LLMs. The file installed, PDF Editor.exe had the following properties:

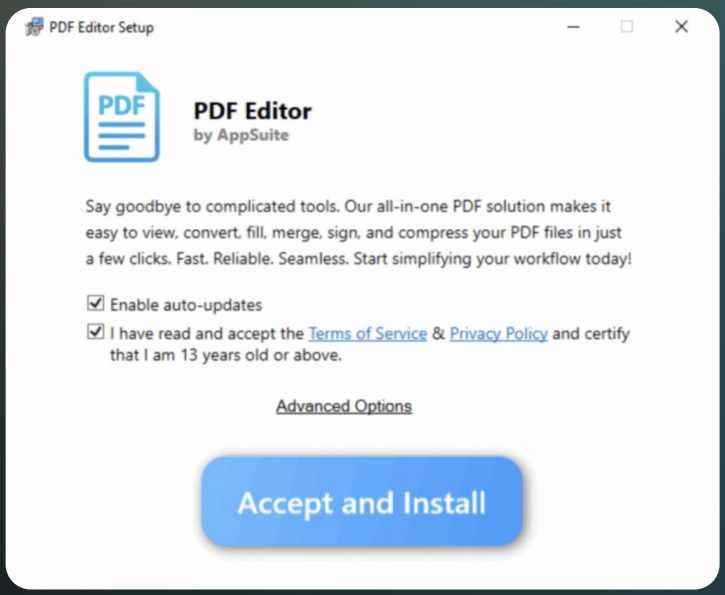
Filename: PDF Editor.exe

MD5: 6fd6c053f8fcf345efaa04f16a-c0bffe

SHA1: 2ecd25269173890e04fe00ea-23a585e4f0a206ad

SHA256: cb15e1ec1a472631c53378d-54f2043ba57586e3a28329c9dbf40c-b69d7c10d2c

When the user executes the installation file, a EULA is first prompted:



It then makes an HTTP GET request to indicate that the installation process has been started. This is sent to the URL: hxxp[://]inst[.]productivity-tools[.]ai/status/InstallStart?v=1[.]0[.]28[.]0&p=PDFEditor&code=EN-US

The next step is that an executable file is downloaded from: hxxp[://]vault[.]appsuites[.]ai/AppSuites-PDF-1[.]0[.]28[.]exe. This is a binary that turns into the actual malware.

After successful installation, it makes two additional GET requests to confirm that all is set.

hxxp[://]inst[.]productivity-tools[.]ai/status/Download%20Complete?v=1[.]0[.]28[.]0&p-=PDFEditor&code=

hxxp[://]inst[.]productivity-tools[.]ai/status/InstallDownloadComplete?v=1-[.]0[.]28[.]0&p=PDFEditor&code

During the setup process, a registry key is also added for persistence, which is executed on startup. It contains a --cm argument that gives executable instructions on how to behave.

Internet records suggest that this campaign began on June 26, 2025, when many of the sites linked to it were either first registered or first known to have promoted the AppSuite PDF Editor. However, the PDF editor was first submitted to Virustotal on May 15.

The –cm have the following different arguments.

--install

--enableupdate

--disableupdate

--fullupdate

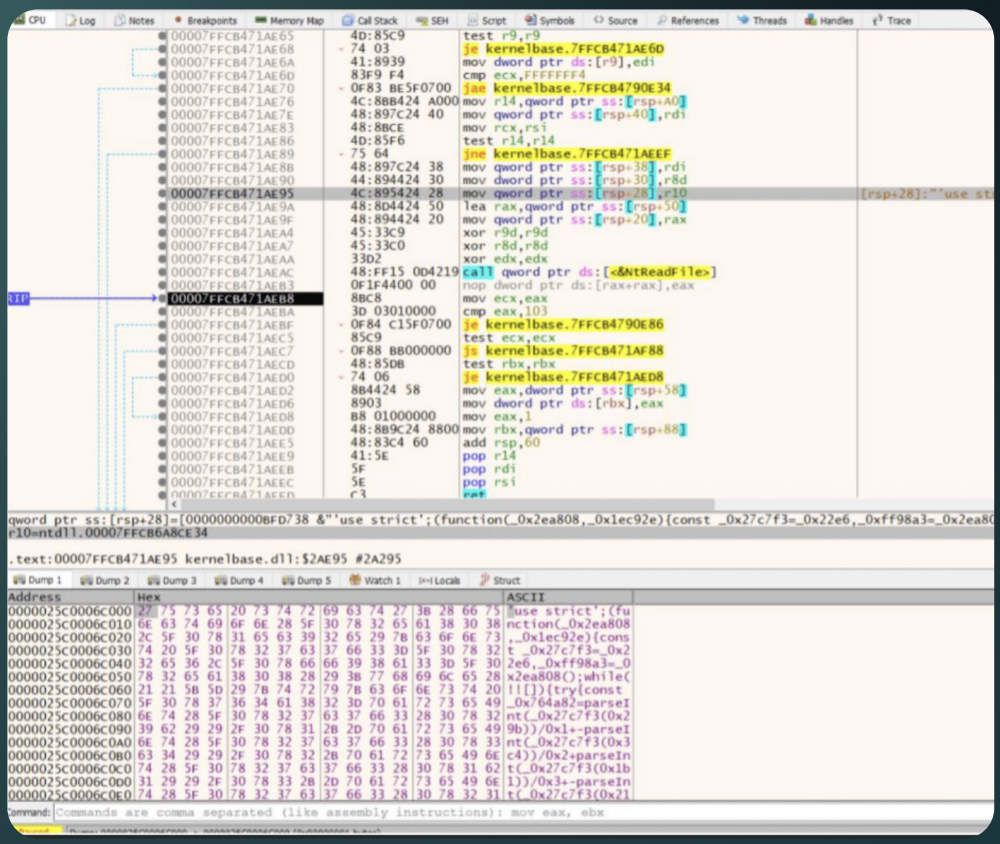
--partialupdate

--backupupdate

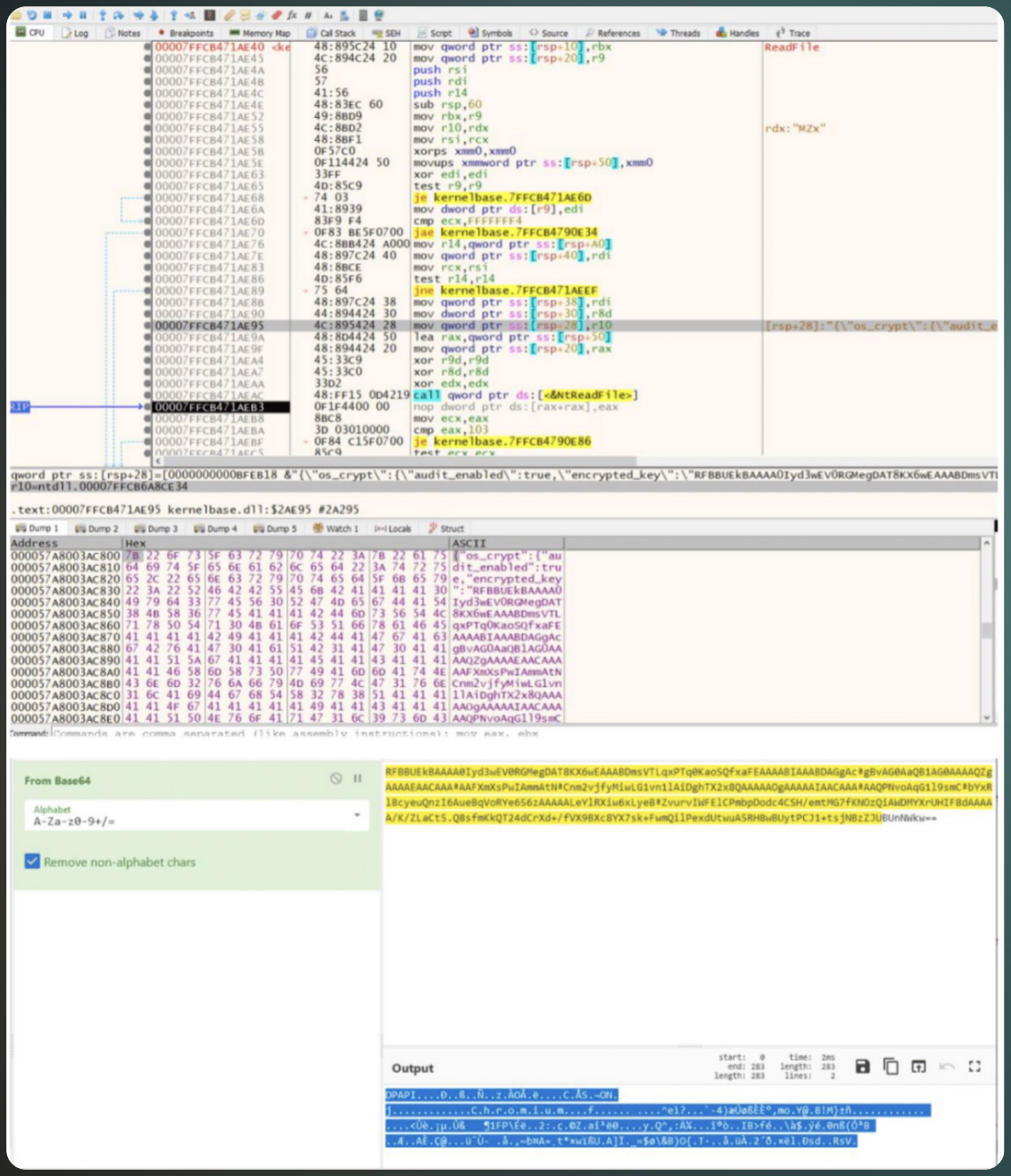
--check

--ping

--reboot



When initialized, Tamperedchef starts to query the web browser's database using DPAPI.



Upon startup, it begins querying the system for different security products. Then it terminates different browsers, likely to access data within them, which is locked if running.

Data traffic to sites that distribute the AppSuite PDF Editor includes referrers from Google Ads campaign codes, suggesting

that the threat actor behind this campaign used Google advertising to promote this PDF editor. The duration from the start of the campaign to the malicious update was also 56 days, close to the 60-day length of a typical Google advertising campaign, suggesting the threat actor let the ad campaign run its course, maximizing downloads, before activating the malicious features.

The threat actor has used multiple versions of the AppSuite PDF Editor app, each signed with certificates issued by at least four different companies. The companies are:

- ECHO Infini SDN BHD
- GLINT By J SDN. BHD
- SUMMIT NEXUS Holdings LLC, BHD
- Byte Media Sdn. Bhd.

The web pages of these companies all appear highly generic and likely AI generated. The companies appear to be nothing more than shell companies established to obtain signing certificates in their names.

An investigation into these companies revealed additional shell companies registered at the same addresses, with similar, generic-looking websites of companies purporting to be in "digital transformation".

These new companies, in turn, also had code signing certificates that pointed to other malicious apps. So, the threat actor behind the malicious PDF editor appears to have a plethora of malicious apps created with the aid of an LLM, along with an infrastructure of fake shell companies and websites to distribute them.

An interesting fact is that the traces of this threat actor go back several years to an old malicious browser extension released under the name "Blaze Media". The threat actor had expanded their operations considerably over the last year, from a malicious browser to a range of apps, likely due to the adoption of AI and LLMs to accelerate operations.

Read more at: Malicious Appsuite PDF Editor Spreads Tamperedchef Malware by scanning the following QR code:

The Use of AI in Cyberattacks

Velocity, Scale, and an Expanded Attack Surface

In 2025, AI has revolutionized software development. New and powerful large LLMs are increasingly being used in the industry. It is only natural that cyber threat actors follow the same path, for the same reasons.

Correctly used, AI and LLMs can be powerful tools in software development, but they also have limitations. "Vibe Coding" lowers the bar for software development, and speeds up the process, but such code is often full of errors and the time gained in writing the code is sometimes lost in bug-fixing.

Alternatively, apps are released full of security holes, as LLMs are still notoriously bad at securing its own code.

We are seeing a similar development among cybercriminals and espionage groups. Using LLMs can make their production considerably faster, but the result is seldom better than what an experienced and skilled human can produce.

Some things that become considerably faster and cheaper to produce using LLMs include writing phishing email texts, building fake web sites, obfuscating code, and generating updated versions of malicious code when the original is detected by antivirus solutions.

Using LLMs to generate texts can give a threat actor the ability to craft convincing spear phishing emails in multiple languages, but the reality here is that these emails often contain all the typical AI hallucinations and mistakes that LLMs have.



An AI-generated text will almost always have a lower success rate than one crafted by a human operator with an understanding of language and local culture, but not all threat actors have access to such individuals. One reason why LLM-assisted phishing emails are often more successful than many written by humans is likely that many cybercriminals have only a cursory understanding of the business texts they attempt to mimic.

Some threat actors are now experimenting with malware that use calls with prompts to LLM to generate malicious commands, so they won't have to include them in the code, where they can be detected. Such novelties are unlikely to have a lasting effect, as the prompts themselves can also be detected. It will nonetheless have an impact on the security tooling out there, demanding a higher sophistication level, and updating to be capable of identifying malicious prompts, for adequate protection.

The sheer volume of email and code an LLM can produce for the same cost as a skilled human operator can also still lead to more successful breaches. The important lesson here is that threat actors use AI for the same reason as industry does, because it does the job more effectively, not because it's better than skilled humans. Correctly used, AI can enhance the productivity of skilled human operators, but not yet replace them.

The AI technology is still in its early stages and it's too soon to predict how it will advance in a few years' time. For now, however, it appears that the greatest threat to cybersecurity isn't highly sophisticated AI-powered cyberattacks, but a deluge of "AI slop": relatively simple and stereotypical attacks that are fast and easy to replicate..

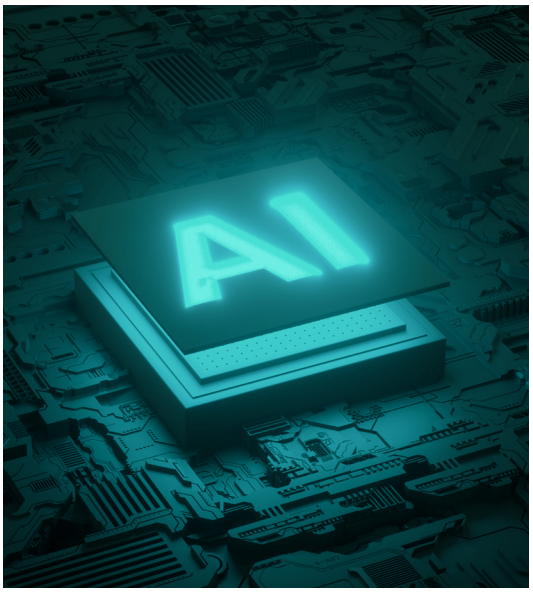
Core security features that focus on specific signatures or patterns, can be crippled by polymorphic malware, but behavioral-based detection remains effective. Detection based on known strings and file hashes can also become overwhelmed by the sheer numbers of new LLM-created projects. The race between offensive and defensive AI in cybersecurity is currently less about sophistication and more about speed and volume.

AI Is Your Friend, If You Use It Safely

The widespread adoption of AI and LLM brings two separate, but linked problems. How to secure your networks from malicious use of LLM and AI, and how to secure your own use of LLM and AI.

Vibe Coding is opening up new possibilities for software developers to quickly realize ideas into proof-of-concept apps that can be tested and developed into new features faster than before.

This doesn't eliminate the need for DevOps, DevSecOps and indeed, human developers. A successful POC still needs to go through the regular development cycle before it can be implemented safely in production.

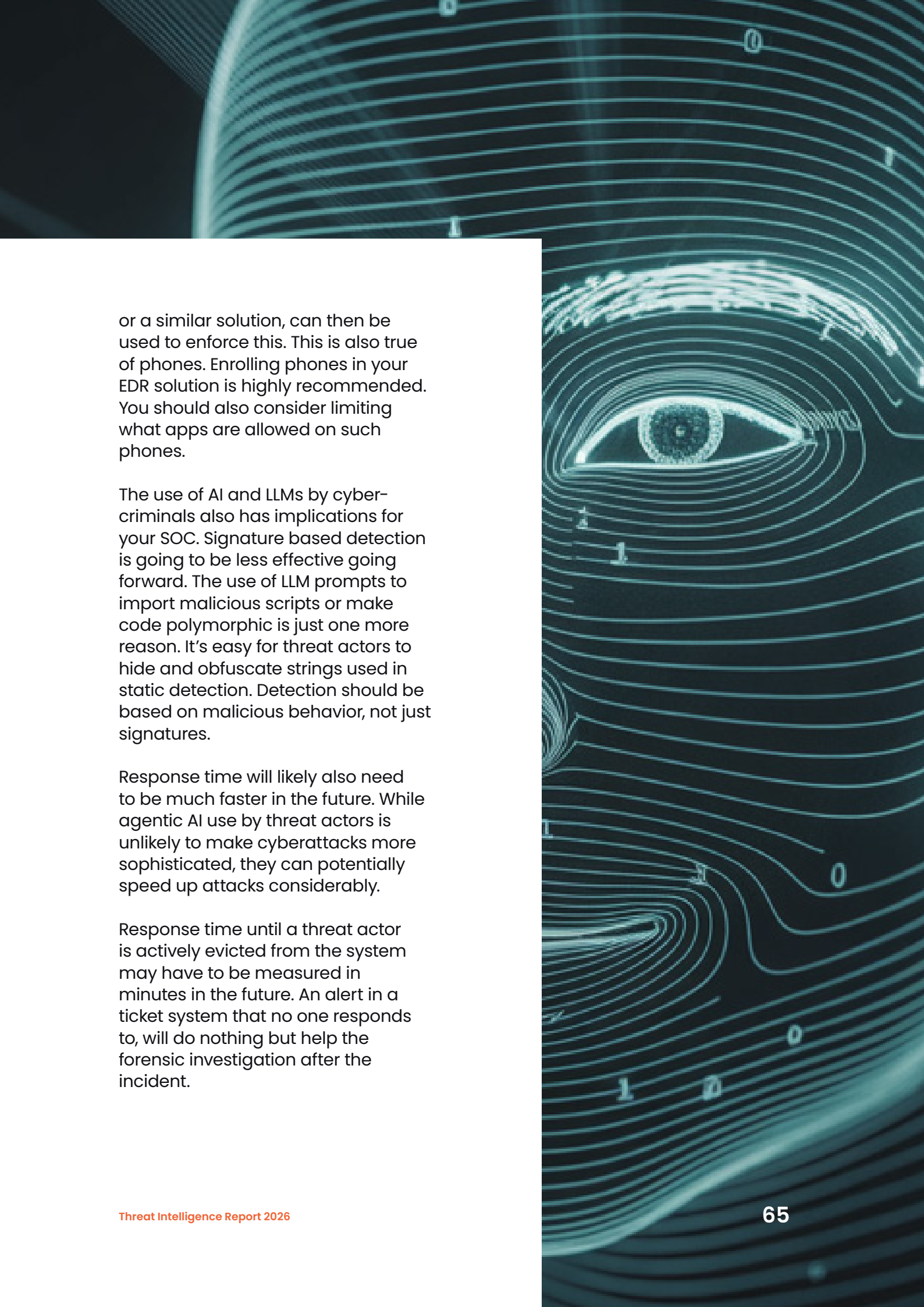


Vibe-coded apps are great for testing ideas, but seldom safe for production.

Incorporating an LLM into your organization's environment also introduces its own security risks. It is vital to carefully weigh the risks of allowing an LLM to ingest your data, even if it is not exposed to the outside. Limiting what data an LLM can access is also required to comply with the EU member states' local implementations of the NIS2 directive.

The use of LLM by cybercriminals also means that it is now easier than ever to produce legitimate looking apps that are actually malicious. Many threat actors have learned how to circumvent trust-based security, by registering shell companies for the express purpose of obtaining code signing certificates to sign their binaries.

The fact that we are now flooded with various vibe-coded apps, both malicious and non-malicious, also means that organization's need to put more thought into what apps users are allowed to use on machines that have access to their network. Ideally, only approved apps available from a company portal should be allowed, and AppLocker,



or a similar solution, can then be used to enforce this. This is also true of phones. Enrolling phones in your EDR solution is highly recommended. You should also consider limiting what apps are allowed on such phones.

The use of AI and LLMs by cyber-criminals also has implications for your SOC. Signature based detection is going to be less effective going forward. The use of LLM prompts to import malicious scripts or make code polymorphic is just one more reason. It's easy for threat actors to hide and obfuscate strings used in static detection. Detection should be based on malicious behavior, not just signatures.

Response time will likely also need to be much faster in the future. While agentic AI use by threat actors is unlikely to make cyberattacks more sophisticated, they can potentially speed up attacks considerably.

Response time until a threat actor is actively evicted from the system may have to be measured in minutes in the future. An alert in a ticket system that no one responds to, will do nothing but help the forensic investigation after the incident.

Securing Your Data in an Insecure World

The Challenge of Knowing When *"The Regular"* Becomes a Threat

The vision of an open digital world, where information flows in a global cloud without interference or borders, appears to be coming to an end. China is using its massive production capability to flood European markets with cheap, effective tech that often contains software with security flaws or hidden backdoors that China can abuse. Recently, Norway found hidden 5G SIM cards in buses bought from China, which could be dialed in from outside to impact the service.

Commercial Chinese-built network devices have been known to route information back to China for years. It's now increasingly the same across the world. The Indian government has enacted laws requiring hosting providers to retain network traffic for up to 6 months for potential government inspection. Everywhere, governments are asserting control over digital information physically stored within the country or passing through it and attempting to leverage it for their benefit. There is a similar suggestion in Sweden, where a number of independent inter-communication service providers can, according to the suggestion, become subject to mandatory judgments by a secret court to retain communication in end-to-end encrypted communication services if the communication is deemed to contain information valuable for fighting organized crime.

The U.S. America First policy, coupled with its readiness to use threats to impose its will on long-standing allies, exemplified by open challenges to Greenland's sovereignty, is eroding Europe's trust in the U.S. This has raised questions about Europe's dependency on U.S. tech. Two events have added momentum to the effort to reduce European dependence on U.S. technology.



The first event is that the new U.S. administration fired several members of the U.S. Privacy and Civil Liberties Oversight Board (PCLOB), leaving the board unable to issue rulings. Efficient oversight by the PCLOB was a key factor in the EU Commission's decision to issue the latest adequacy decision and sign the Data Protection Framework with the U.S., enabling personal data transfers and processing in the U.S. without requiring additional safeguards from data controllers. This raises concerns over the adequacy decisions and the data privacy framework's longevity and, in consequence, to what extent that personal data can be lawfully processed by U.S. cloud providers in the future.

The second event is the U.S. sanctions on key personnel in the International Criminal Court (ICC) over the ICC's refusal to drop the war crimes charges against Israel officials.

Another significant consequence is that U.S. sanctions on Russia prevent the issuance of new licenses for cloud products in the Russian market. While such measures against Russia may be in line with Europe's interests, similar restrictions could be imposed on other nations at the U.S. government's discretion.

Today, there are very few reliable alternatives to U.S. IT technologies. The massive U.S.-based hyperscalers are inexpensive and effective. They also have the resources to continually identify and patch vulnerabilities in their systems. U.S. tech giants themselves have shown no interest in being drawn into any conflict that would force them to act against the interests of their European customers. However, as they have testified, they can be forced to obey the U.S. government.

There are several promising projects today with a stronger focus on Europe and the EU. The Digital Europe Programme (DIGITAL) is an EU funding program that supports the deployment of digital technologies to businesses, citizens, and public administrations across the EU, with a focus on European solutions. Most of these projects are in the research or evaluation phase and are not ready to be scaled up or to compete with U.S. services. Today, the road to an independent European tech industry that can rival the U.S. is still very long.

Many of the European startups referenced are open source programs. A problem with open source alternatives is that they can be vulnerable to infiltration by threat actors. For example, the malicious backdoor found in XZ Utils was the culmination of a three-year-long effort to infiltrate and compromise this open source project.

Another threat to an independent European software industry is that U.S. tech giants have the financial muscle to buy promising European startups that could pose a threat to them. Even if these European initiatives are successful and can eventually be scaled up, they will likely not be able to break European dependence on key U.S. IT technologies for at least 5-10 years.



The adoption of AI in enterprises introduces new risks to data integrity. LLMs create an additional attack vector that can lead to data compromise if access controls and usage policies are not strictly enforced. Virtually all LLMs available now are owned by either U.S. or Chinese companies.

Not Taking the Regular for Granted

Using hosting providers and technology from countries such as India and China entails an obligation to conduct ongoing risk assessments for enterprises seeking to capitalize on the lower operational costs. Enterprises need to understand the trade-offs associated with out-sourcing critical IT functions, including increased risk, a larger attack surface, and susceptibility to threats that may not exist in lower-risk countries with higher operational costs.

The fact that the U.S. government has shown itself willing to use its power over U.S. tech giants to cut off individuals within organizations like the ICC from American IT services is a cause for concern. Until now, the widespread adoption of a technological ecosystem built on U.S. tech giants has been, in part, based on trust, and broken trust is not easily repaired.

Organizations should weigh risks against one another. U.S. cloud services offer effective, affordable solutions, but can place your data under U.S. government control, which should, regardless of what origin a piece of technology has, always be considered and, depending on context, classified and managed as a potential risk. Enterprises with a global footprint often need to connect their networks to high-risk nations to do business, but doing so safely requires careful planning.

Microsoft is reportedly exploring a new model that would allow several European hosting providers to run Azure independently on a licensing model.

This could potentially put European customers' data outside U.S. legislation. If implemented correctly, this could alleviate some current risks, but the outcome of these negotiations will still determine the final result.

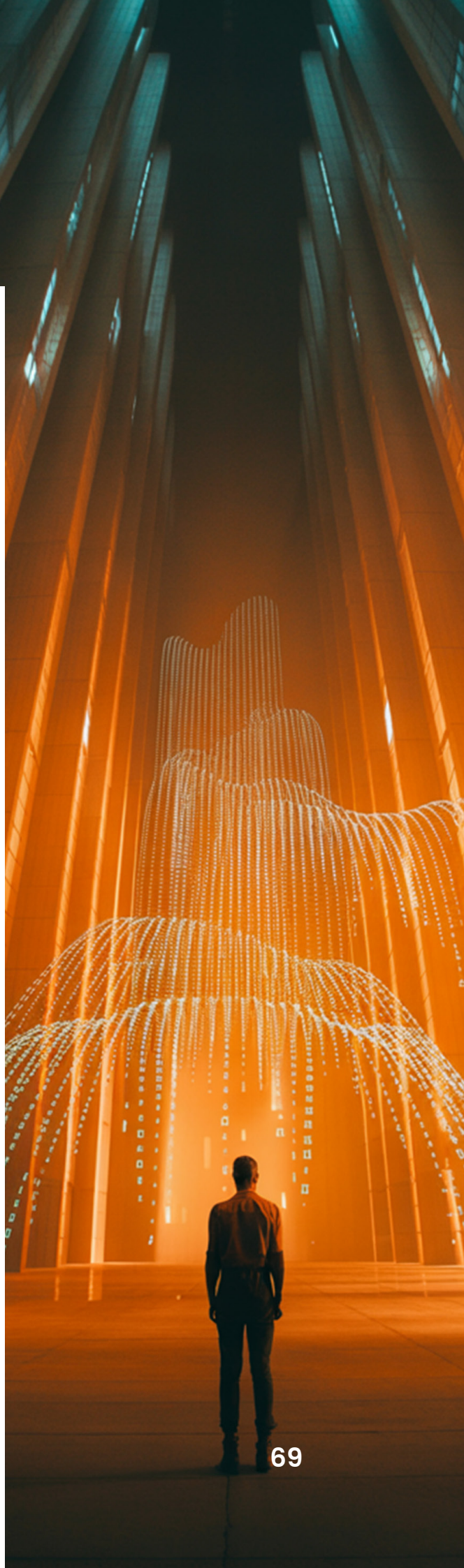
The most significant potential impact of an open conflict between the U.S. and Europe is that the U.S. government can, and has already demonstrated a willingness to, impose sanctions on both individuals, as in the case of the ICC, and on entire nations, as with Russia. Given the widespread adoption and extensive capabilities of U.S. cloud services, sanctions that cut off individuals or nations from these services could force organizations and governments to implement alternative solutions on extremely short notice.

The risk that something like that would happen in Northern Europe is hard to quantify, but imposing sanctions on entire European nations would be a "nuclear option" strongly resisted by the U.S. tech industry, as it would likely devastate its future sales in Europe. Truesec assesses that the risk of this occurring is small in the current climate, but that, given the unpredictability of the U.S. administration, this assessment can change in the future.

Outside of preparations for the extreme scenario of a complete cutoff of U.S. services, organizations can take steps to secure their data from compromise by foreign governments when using U.S. tech or storing data outside Europe. Data governance is key to protecting sensitive data, regardless of whether the threat is from a physical site in a high-risk country, training an LLM on your data, or software or hardware products from potentially hostile countries.

On-prem solutions offer greater control over your data than cloud solutions. This can also be extended to EDR and log handling. Network segmentation, permissions, and identity management based on clearly defined roles can help secure environments against data loss from cyber espionage and LLM leakage. Organizations must evaluate risks, assess their threat profile, and understand business needs. Cloud or on-prem, U.S. or Europe, all the options come with their own pros and cons, whereas each organization weighs them differently. Despite the risks, continuing to use current U.S. solutions, whether cloud or on-prem, remains the safest and most efficient option for most organizations in Europe today.

Geopolitical risks are now affecting cybersecurity, so staying on top of international political events and interpreting their implications is also vital for cybersecurity. Threat intelligence is more important than ever.



Hybrid Warfare

At the “Folk och Försvar” conference on January 25, 2025, the Swedish Prime Minister stated: “Sweden is not at war. But neither are we at peace.” This sentiment reflects a reality where conventional war is absent, yet hybrid conflict is pervasive. While NATO is not engaged in open conventional warfare with Russia, the relationship is adversarial.

Hybrid warfare refers to conflicts that blend conventional military force with non-military tools, such as cyber-attacks, disinformation campaigns, and economic pressure. Unlike conventional warfare, which primarily relies on military power, hybrid warfare leverages the entire spectrum of political, military, economic, social, informational, and infrastructural domains to achieve strategic objectives.



The attempt to achieve long-term objectives through the synchronized use of three or more instruments of such powers while deliberately remaining below the threshold of declared war or *casus belli* is "hybrid war".

According to this definition, a single cyberattack does not qualify as hybrid war; only their orchestrated fusion into a unified campaign across several domains does. Being in a state of hybrid war introduces new cybersecurity challenges, as the cyber domain becomes a focal point for foreign influence and disruption. It is therefore paramount that we incorporate what we understand about hybrid war and its manifestations in cyberspace when we consider our future defensive requirements.

Malign use of cyberspace has existed for decades, particularly within economic crimes. What hybrid warfare adds is a political dimension: adversaries exploit vulnerabilities to create fear, confusion, and mistrust. Confrontations in hybrid conflicts are often asymmetrical, striking where the opponent is weak. For example, the West enforces economic sanctions, while Russia exploits open and free societies to spread propaganda and fear. If cybersecurity of key government institutions and civic functions is lacking, adversaries will target it, not necessarily for direct military gain, but to erode confidence and to cultivate FUD in sovereign populations. This FUD can, in turn, be leveraged in disinformation campaigns to erode the democratic foundation of individual countries and the unity of allies.

Shaped by Russia's long-standing use of cyber operations and information warfare, which began well before the full-scale invasion of Ukraine in 2022, the cyber domain is a main front in this conflict. In fact, Russia has employed these tactics since at least 2008, as seen in Estonia. And Sweden has experienced pressure from Vladimir Putin's strategic aspirations before joining NATO.

The Nordic region is a case study of this development, and recent events have demonstrated Russia's willingness to employ tactics such as disruptive cyberattacks and information domain warfare. Denmark and Sweden will hold national elections in 2026, creating opportunities for information operations, disruptions, and cyber sabotage that could undermine trust in democratic processes. The DDoS attacks during Denmark's municipal elections in November 2025 foreshadow what may come. Simultaneously, Nordic countries are becoming key hubs for defense production supporting Ukraine, making them prime targets for espionage and sabotage.

As tension rises, the risk of escalation grows. Political leaders warn that open war between NATO and Russia is not inconceivable within a few years. Ukraine's experience shows that once this threshold is crossed, cyber defense extends beyond cyberspace: protecting against destructive malware and even kinetic strikes against critical infrastructure such as server farms might become a reality for cybersecurity. Preparing these scenarios is essential. Robust cybersecurity and resilience can deter adversaries and reduce the likelihood of escalation.

Outlook 2026



AI Will Not Change the Game, but It Will Change the Pace

Two factors will shape cybersecurity and cyber threats in the coming year more than anything else: geopolitical challenges and the continued adoption of artificial intelligence.

It is easy to be misled by the venture-capital-driven hype around various AI initiatives, but beneath the hype, fundamental changes in IT technology, driven by AI, will continue regardless of whether the financial growth expectations surrounding AI are sustainable.

In 2026, Truesec expects more threat actors to incorporate the use of LLMs and AI-based solutions into their attack chains. We do not expect anything like true agentic AI to replace human operators in complex intrusions; instead, we expect skilled threat actors to use AI to automate tasks, making them cheaper and faster to perform.

This will not fundamentally change the challenge facing defenders, but it will likely require faster response times. A ransomware operator that uses AI to automate parts of the attack chain may reduce the time from initial breach to full encryption from days to hours, or even less than an hour. Response times for defenders need to match this speed.

Using AI to automate attacks can also reduce the time and money required to breach an organization. This, in turn, will enable a cybercriminal business models focused more on mass ransomware attacks targeting smaller enterprises than those typically targeted today. Cost-effective cybersecurity solutions for smaller organizations will likely become more necessary in 2026.

The widespread adoption of AI will also make it an attack surface. LLMs and other AI solutions exposed to the internet will be targeted by prompt-injection attacks. The use of online LLMs accessed through web browsers will be exploited by owners harvesting the user's data, but even offline LLMs can become a tool for an attacker.

For years, the cybersecurity industry has preached network segmentation and tighter identity management as key to improving cybersecurity. Now, some organizations are undoing this work by allowing all their company data to be ingested into a company LLM.

In 2026, Truesec assesses that threat actors will begin experimenting with using a company's AI to map their victims' environments once they have gained a foothold. Once a threat actor has gained access to a patient zero and stolen their identity, they can contact the company AI. What better assistant in determining where the most vital data is stored and how it's secured than the victim's own AI? How do we ensure our AI does not become a single point of failure or even the ultimate insider?

Globalized Cybercrime

Ransomware has, for all intents and purposes, been a problem originating in Russia. But now cybercriminals from around the world collaborate on sophisticated ransomware attacks.

Ultimately, organized cybercrime, like all crime, is tied to the societies it springs from. When ambitious people with the right skills see no legal way to achieve their ambitions, they often turn to crime. The most corrupt societies are often also the most crime-ridden. The financial markets and the ways leaders of the world can instill hope in their citizens' economic future will also determine the growth of organized cybercrime.

Many developing countries, while often plagued by corruption, have now attained a level of wealth that makes owning a computer within reach. This means more technically proficient computer users, and as a result, potentially more hackers. As we know, cybercrime, unlike other forms of organized crime, has a global reach and requires no physical foothold in the victim's country.

Even in the Western world, where many young people now believe that achieving the same standard of living as their parents is not within reach, there has been a rise in cybercriminals who are often young and cynical. This is also an area where foreign adversaries' information operations can affect cybercrime. Divisive and demoralizing state-sponsored propaganda is designed to give rise to more disillusioned youth who sometimes turn to cybercrime.

Geopolitical developments will shape not just hybrid threats and cyber sabotage but also organized cybercrime. The current trend is worrying. While the international community's united action against organized cybercrime is under strain, organized cybercrime is becoming more globalized than ever.

Predicting the future of the geopolitical landscape is beyond the scope of a cyber threat landscape report, but wars, conflicts, and trade wars will likely trigger a global financial downturn unless they can be contained. If this comes to fruition, it will likely fuel more cybercrime.



War and Innovation

Large wars can trigger significant innovation. The logic of war reveals what military and technological concepts have become obsolete, and which are the new paradigms. The war in Ukraine has revealed that missile and drone technology is more critical than either side believed before the war.



On all sides, nations and entrepreneurs now scramble to learn from the experience of those involved in the war and to invent their own concepts. Drones and drone defenses are evolving rapidly.

Cyber espionage is already an essential part of this new arms race, and cybersecurity must try to keep up. This is especially important, as many of the organizations at the forefront of this new technology are small startups with significant innovations but fewer resources to invest in cybersecurity.

The Nordic countries are now among the most critical hubs in the European defense sector. Ensuring that startups engaged in cutting-edge defense-sector technology have the proper cybersecurity focus will be a critical concern for our own security in 2026.

Software Development Is Becoming the Weakest Link

For years, most cybersecurity efforts have focused on those with the least information: users. The average user in a corporate environment today has a fairly locked-down machine with few options that could compromise cybersecurity.

Software developers, sometimes with included IT administrative tasks, are trusted to be more knowledgeable and therefore have far greater permissions to conduct actions that could potentially compromise security. They also require elevated permissions to do their jobs, but in many cases, they have higher permissions than needed, often based on trust, which can make a single mistake fatal.

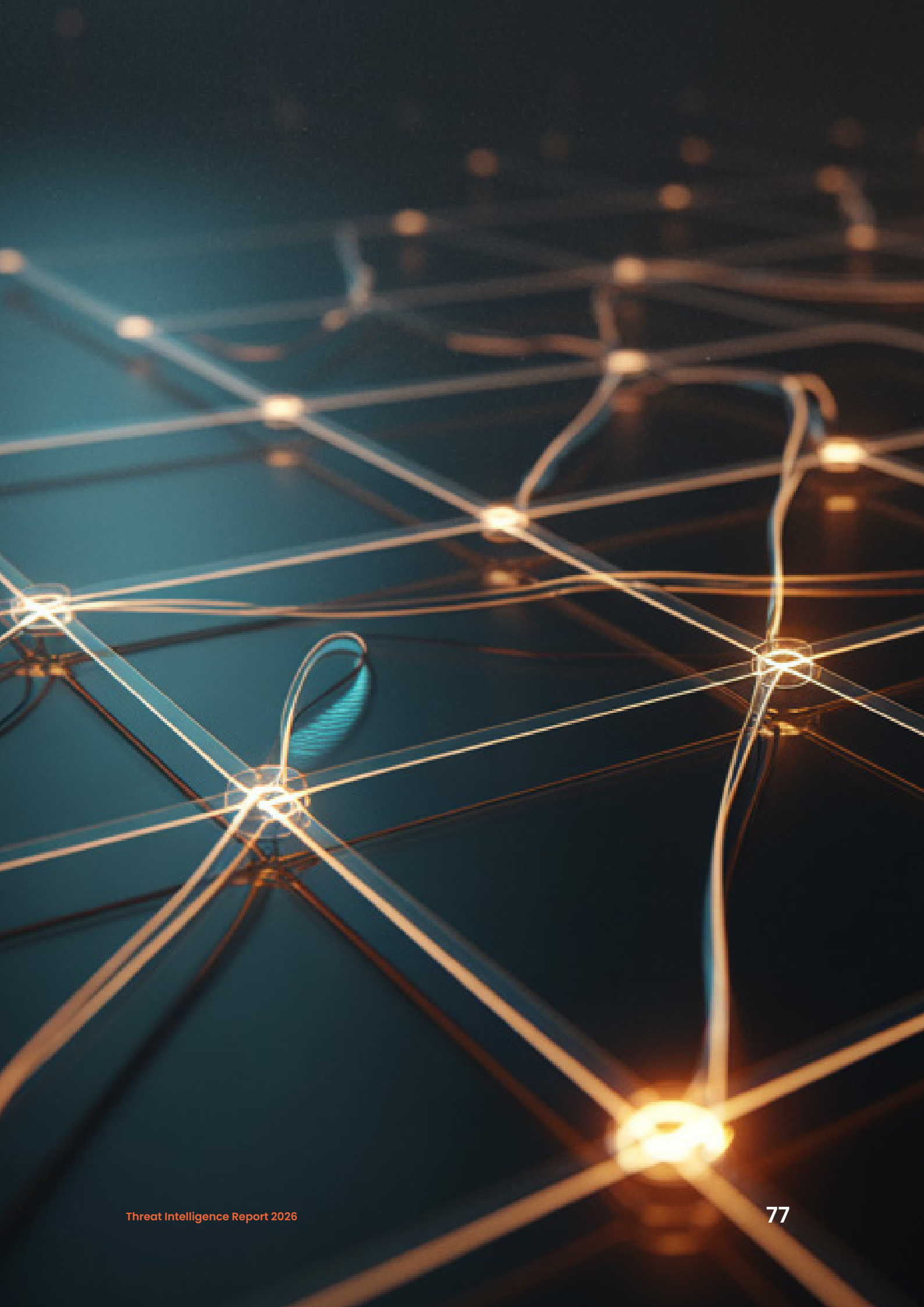
These permissions and access to software pipelines have now put them in the crosshairs of a growing number of threat actors. A wide variety of attacks, from sophisticated social engineering to mass supply chain exploitation, aim to compromise software developers.

The epicenter of this is the ungoverned part of the open source software community. Large parts of software development today are heavily dependent on open source code projects. Most such projects, in turn, contain numerous dependencies.

As a result, large parts of the code used in most software products are maintained with less security than warranted, given how many users can be affected if the code is compromised. Some projects are arguably better from a security standpoint than others, but the vast majority place nearly zero emphasis on security.

Until the ungoverned open source community finds a solution to this problem, Truesec assesses that the rise in cyberattacks targeting software developers in general and open source projects in particular will continue and may even accelerate. Some forms of gatekeeping and improved security for such hubs may eventually be required, even if that means introducing fees to finance them. This is very difficult to do, however, as there is no structure or governing entity. The entire concept of open source is based on freedom and creativity.

Just as streaming services reduced the problem of pirated media, which was often riddled with malware, something similar may be required to address the massive scale of targeting of open source code-sharing hubs, which are increasingly vulnerable to a growing number of threat actors.



Security Will Be Everyone's Concern

As the boundaries between cyberspace and the real world blur, so do the boundaries between cybersecurity and physical security. With improved technical cybersecurity, more threat actors will try to "hack the human" instead of the machine.

Social engineering is one of the oldest tricks in the book, but it's also constantly evolving. AI technologies, such as deepfake images, will likely further enhance the success of social engineering attacks in the coming year.

As our lives become increasingly digitized and publicly shared on social media, it becomes easier to find information about individuals and to use it to gain their trust. To meet the challenge posed by threat actors using social engineering to trick us into lowering our guard and granting them access, it will be vital to make cybersecurity everyone's business in 2026.

If we don't invest in the human layer of cybersecurity, it won't matter if the technical controls are best-in-class. First-line defenders, such as help desks and IT support, are a vital part of cybersecurity, as they control network access and should be treated as part of the cybersecurity team. That means investing in their knowledge and empowering them to be vigilant.

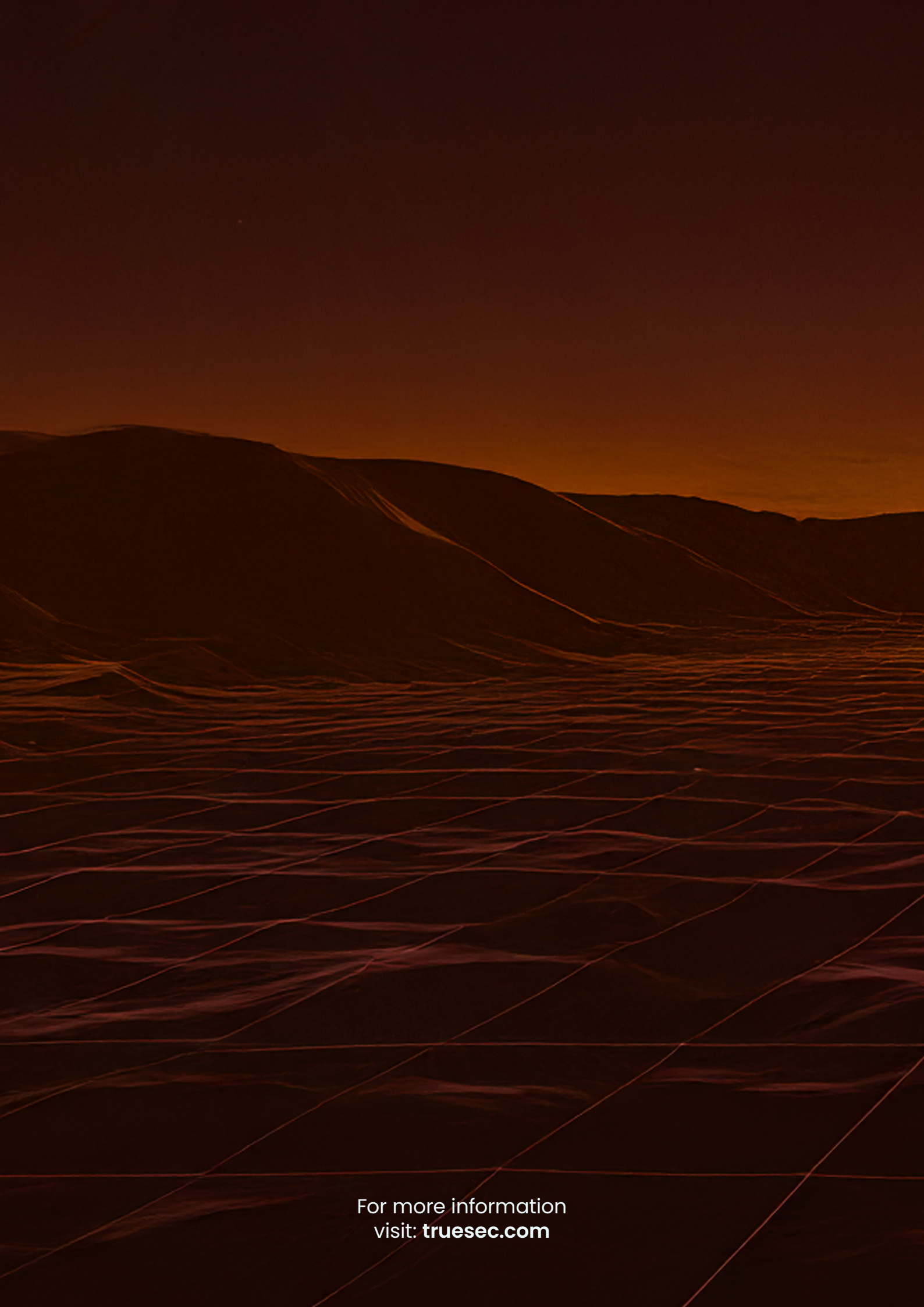
Not everyone needs to be a security expert, but raising awareness and fostering a security-aware culture will be key to improved cybersecurity in the coming year.



Prevent Breach & Minimize Impact

For more information visit: truesec.com





For more information
visit: **truesec.com**