Threat Landscape

↘ 2023/2024

The full picture of cyber threats in a year of transformations spurred by the adoption and evolution of artificial intelligence technologies. And the predictions and trends of what 2024 holds for cybersecurity.

///AXUR

What will you find in this report?

Content Index

A message from Axur

A message from Axur

We know that threats change from year to year. The scale and pace of change vary, of course, but there is always something new that warrants our attention. Some of these changes remain and become trends, but others are just temporary anomalies.

Following a slight decline in ransomware attacks in 2022, the year 2023 saw this threat reignited, along with the many challenges it poses.

This resurgence in ransomware attacks was accompanied by two methods of access: supply chain attacks and insider threats. Many of the new attacks take advantage of business connections and technological ecosystems to reach targets far from the point of entry. It's even worth reflecting on whether the narrow concept of an insider threat still makes sense when there are so many networks and connected environments.

Meanwhile, we have been experiencing transformations spurred by the adoption and evolution of artificial intelligence technologies. In our cybersecurity environment, this technology can generate new types of attacks or enhance old threats, as is already happening. At the same time, we need to look for measures that use AI to safeguard data – and this depends on us, who know the need to detect and prevent new attacks quickly and the lack of specialized professionals for this task.

We hope our report helps you understand the situation we are in and shed light on the ideal path.

Thiago Bordini
Head of Cyber Threat Intelligence | Axur

Executive Summary

Powered by Axur's technology and intelligence expertise, this report gives you a snapshot of the cyber threat landscape of 2023.

Ransomware

The drop in activity by ransomware operators in 2022 was reversed this year. Attacks have resumed and are now incorporating new social engineering approaches and attacks on third parties (supply chain).

Although they are still called ransomware, some attacks have also left file encryption in the background, preferring to bet on a threat based on the regulatory and legal costs that can arise from a data leak.

Credentials in the crosshairs of attackers

Access credentials theft remains high,

Axur monitoring detected 4.2 billion leaked credentials in 2023,

continuing the trend established with the use of credential stealer malware and other attacks to recycle credentials stolen in data leaks. The adoption of multi-factor authentication remains an important requirement to hamper the use of these credentials.

Increase in debit and credit card leaks

We have detected a significant increase in the sharing of card data among criminals. Our monitoring identified that

> more than 13 million cards were leaked, a 265% increase from 2022.

Most targeted sectors

Criminal activity on the Deep & Dark Web was mostly concentrated in the retail, finance, and technology sectors, which accounted for 77% of suspicious incidents. In phishing detections, the share of these three sectors was even higher: 90%.

Artificial Intelligence

The use of artificial intelligence allows criminals with little programming knowledge to produce malicious artifacts or configure pre-existing tools easily. Large Language Models (LLMs) have been used to automate interaction with victims in social engineering attacks via messaging and communication applications.

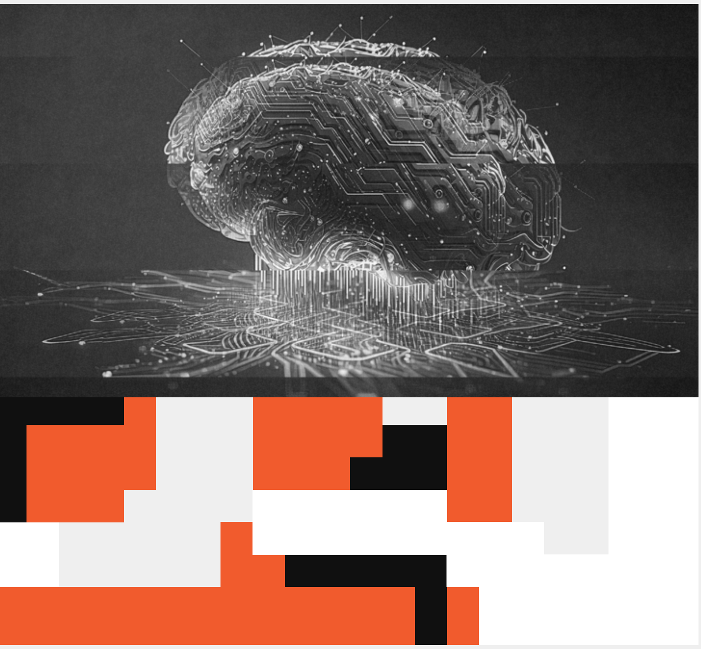
Geopolitical Instability

The conflicts between Ukraine and Russia and Israel and Hamas have instigated groups of hacktivists who target companies and organizations associated with any country that speaks out in favor of the nation they consider an enemy. In addition, the actions of these groups tend to be more unpredictable than attacks carried out by criminal groups motivated solely by financial gain.

Phishing

The retail and financial sectors are the most targeted by phishing attacks.

> Over the course of 2023, we identified more than 31,000 phishing pages.



Artificial Intelligence

The possibilities involving the use of AI tend to enable new forms of fraud and attacks. On the other hand, AI can be a fundamental part of advancing cyber threat intelligence, whether in organizing information, speeding up processing, or improving monitoring.

Social Engineering

Social engineering proved to be a major challenge in the attacks that occurred in 2023. Attackers are approaching partners and suppliers, expanding the number of viable channels to gain access to a target.

The use of threats of physical violence can also be even more surprising.

2023

February

→ The Cl0p ransomware gang exploits a vulnerability in the GoAnywhere software and threatens to expose the data of more than 130 companies

→ The online social platform Reddit reveals that it was the target of a sophisticated social engineering attack that gave attackers access to documents, code and internal systems

March

→ The password manager application LastPass reports that an incident in 2022 leaked users' encrypted vaults. Blockchain analysts believe that criminals are accessing these vaults to obtain private keys, which allowed the theft of more than $40 million in crypto assets

→ A bug in ChatGPT leaks users' chats into the history of other users, giving them access to chats that belonged to third parties

April

→ A ransomware compromises the systems and customer information of Western Digital, a manufacturer of data storage solutions. They had to take the My Cloud service offline for ten days

→ 3CX, a business communication solutions developer, reveals that criminals accessed the company's systems and included malware in the download of its software through the official distribution channel

May

→ Eyewear manufacturer Luxottica confirms an incident of leaking personal data of 70 million customers

June

→ Cl0p exploits a vulnerability in MOVEit Transfer software to compromise over 2,000 companies. The attack affected banks, hospitals, universities, and public organizations, mainly in the United States

September

→ U.S State Department reveals that emails were compromised by Chinese hackers who exploited a flaw in Microsoft cloud

→ Caesars Entertainment and MGM are attacked by ransomware associated with the Scattered Spider group paralyzing operations. MGM Resorts refused to pay the ransom, leaving the company offline for 10 days and with an estimated loss of $100 million. Press reports and regulatory information estimate losses at $15 million for Caesars and $100 million for MGM

→ Flaw in Google Bard exposes user conversations with chatbot in search results, creating a problem similar to the one faced by ChatGPT in March

October

→ Identity services provider Okta announces that it has suffered two cyber attacks

→ Hackers from the Russian group Sandworm trigger a new power outage in Ukraine after using wiper-type malware to erase all the data and software from a power generator's systems

November

→ Ransomware group LockBit claims to have obtained a 1.5 TB data package containing 24 years of information from Canadian government officials

December

→ Kyivstar, Ukraine's largest mobile operator, suffers a cyber attack that causes instability in its services. The attack was attributed to a Russian intelligence-linked group

Cybersecurity Overview

Cyber attacks have evolved a lot in recent years. With advanced threats and ransomware groups known to move laterally within corporate networks, it seems like we have seen it all. The migration to the cloud, which ended up being a hasty operation for many companies, has also left victims along the way.

With the knowledge we have of these risks and cyberattacks, which horizon deserves our attention?

There is a movement to integrate cyber risk with business risk. This perspective had already been explored by some experts, but it has emerged as the only possible path forward given the magnitude of the losses – particularly when the attack paralyzes the entire company or generates a million-dollar fine due to personal data leaks.

In practice, cyber risk becomes much broader and subject to certain rules that previously only existed for so-called traditional risks.

The Biden administration's Cybersecurity Strategy, in the United States, is largely an interpretation of this perspective, as it understands that software developers and service providers must be held accountable for certain failures – just as in other sectors.

There is also a more intensive search for ways to dilute the risk bill with cyber insurance. The Swiss Re Institute estimates that the cyber insurance market will more than double in size in four years

and reach $22 billion by 2025.

But this is by no means a carte blanche that exempts the adoption of safe practices. Insurance does not cover secondary damages and losses, such as the loss of trust from customers and suppliers. In addition, risk pricing tends to benefit companies that operate responsibly and seek to protect their business.

Insurers are already keeping a close eye on the controls that companies adopt or fail to adopt in order to determine the value of premiums.

On the government side, we have seen cases of American and Australian authorities seeking to hold security managers themselves responsible for failures in companies. Although the regulatory base is still being built, the message that regulators want to send is clear: it is no longer feasible to simply take the risk.

We enter 2024 unsure of how the courts will handle this issue.

Be that as it may, what drives these movements is the maturation of the sector. The scale that balances security and innovation begins to seek equilibrium instead of prioritizing evolution at any cost. As digital services are everywhere, directly or indirectly, digital risk "contaminates" others, just as other risks also contaminate digital.

In 2023, large-scale cyberattacks managed to hit hundreds of companies that had a single point in common. This was the case with the attacks involving MOVEit Transfer,

GoAnywhere, and 3CX. From financial institutions to universities, everyone found themselves equally vulnerable.

Ransomware:

The attacks that exploited vulnerabilities in GoAnywhere and MOVEit Transfer, authored by the Cl0p group, are possibly the most striking examples of what ransomware was like in 2023: aggressive, mass actions. Criminals bet on efficiency, prioritizing threats involving the exposure of stolen data over encryption.

In countries that have passed data protection laws, it can be more difficult to overcome a leak of personal information than the purely technical obstacles that arise from data encryption. If the fine that the company can receive is significantly higher than the amount charged by the scammers, file encryption is no longer the decisive factor in paying the ransom.

Although before it was even possible to talk about triple extortion (encryption, data exposure, and DDoS or other threats), now we have cases of ransomware without the data encryption that has marked this type of fraud.

Ransomware response plans dedicated to data recovery and protection fail to avoid the fines and other regulatory penalties inherent in data exposure.

A case that clearly illustrates this shift in tactics was conducted by ransomware gang ALPHV (also known as BlackCat), which reported a victim to the Securities Exchange Commission (SEC), the U.S securities regulator. The criminals alleged that the company had not complied with its legal obligation to disclose the breach of its systems to the regulatory authority.

As part of this scheme, ransomware groups can spread false claims about the attacks they carry out on their leak sites on the Deep Web. Even if no attack has actually been carried out, it puts pressure on companies and can even damage a brand's image.

- Variant of the CryptoMix ransomware.
- Active since: 2019
- Country of origin: Russia
- Most targeted sectors: various sectors and organizations
- Motivation: financial

- Ransomware-as-a-Service (RaaS) model
- Active since: November 2021
- Country of origin: Russia
- Most targeted sectors: various sectors and organizations
- Motivation: financial

In situations of ⚠ unfounded threats, it is important that companies are able to quickly assess their environments and take a firm stance on the falsehood of criminal allegations.

Of course, traditional double extortion attacks (encryption and data exposure) remained the norm. In any case, the new approaches worked for criminals, and ransomware groups returned to higher revenues in 2023 after experiencing a decline in 2022.

The technical sophistication of cyberattacks, on the other hand, remains closely linked to traditional tactics. Social engineering continues to be one of the biggest risks, but this time it also affects employees from third-party suppliers. The group of criminals known as "the Com" (or Scattered Spider), associated with the aforementioned ALPHV, also stood out with these tactics for their successful social engineering attacks against IT service providers (which led to the incident at the Caesars and MGM casinos) and for using threats of physical violence in their communication to victims.

The ransomware-as-a-service (RaaS) model continues to be responsible for many attacks, as it leads to more diffuse and diverse operations by these groups. In RaaS mode, many criminals can join the operation as affiliates. LockBit is a good example of this, as one of the most actives groups of the year.

- Ransomware-as-a-Service (RaaS) model
- Active since: September 2019
- Country of origin: Russia
- Most targeted sectors: professional services, transportation, manufacturing
- Motivation: financial

While RaaS is not exactly a new thing, it is still accurate to say that many companies suffer ransomware attacks for getting the basics wrong, such as not applying software updates with security patches or neglecting identity and access management. Many of them only realize they lack a business continuity and disaster recovery plan after the attack has happened.

That said, any scenario in which the revenue of ransomware groups is on the rise is highly unfavorable. Considering the high degree of professionalism of these criminal organizations, resources can be reinvested in criminal action, either by recruiting new members or creating new artifacts and tools that make it difficult to detect and attribute the activity.

Artificial Intelligence

The maturing of digital technology and the consolidation of attack tactics have not erased innovation completely, of course.

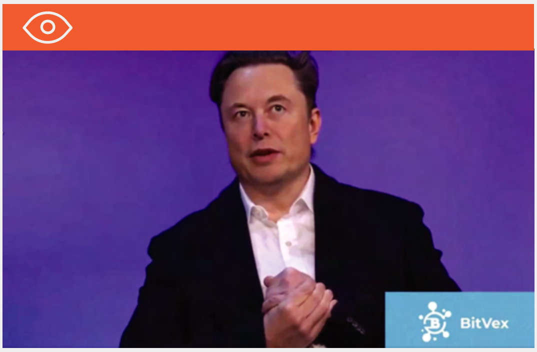
The year 2023 was marked by a significant advance in machine learning and artificial intelligence algorithms.

As the deep learning approach is very versatile, attackers can use this technology in a wide variety of attacks. In 2023, we have already seen the following attacks:

Deepfakes: Manipulated images and voices have been used in some contexts. One example is fake videos that promote cryptocurrency scams using celebrities such as billionaire Elon Musk and Ethereum creator Vitalik Buterin. The videos use images of these executives at events, but the original speeches are replaced by an AI-synthesized voice. The images are only altered to ensure lip sync, which is another function of this type of AI.

The Axur Research Team has also observed cases where AI-manipulated images – for example, those that add movement to static images – have been used to circumvent remote biometric authentication systems. Although this type of authentication usually requires a photo or video captured with a smartphone camera, criminals can use modified apps to send AI-manipulated images and mislead the system.

Finally, the press has been reporting situations in which deepfakes were created by students to tarnish the image of their schoolmates. Even though these situations do not have an immediate impact on corporate security, they do raise the alarm about the possibility of deepfakes being used in conflicts within organizations or as an instrument to sully the reputation of executives.



Social Engineering: Just as companies see the possibility of using AI to automate customer service processes, criminals can use large language models (LLMs) to create robots that interact with victims in social engineering scams.

In these cases, the scammer's approach is usually more indirect than in traditional phishing, requiring the victim to be gradually convinced.

From a fraud perspective, the advantage of this more personal interaction is that the victim becomes more involved and more susceptible to falling for a narrative that would have no effect in an impersonal context. The disadvantage for the criminal is the work involved in maintaining several conversations in parallel, as the fraud is not applied to just one person at a time.

AI-enabled response automation solves this problem for criminals. We have observed that certain approaches by criminals on messaging apps (such as WhatsApp) have used this mechanism to speed up interactions with victims after mass messages have been triggered.

Codes and automation: LLMs have great potential for automating or drafting solutions to programming tasks. For the world of cybercrime, this means that less skilled agents can use these tools to compensate for their lack of technical knowledge.

Commercial AI tools usually have restrictions to prevent them from producing malicious code. However, there are many loopholes allow what is commonly called jailbreaking of artificial intelligence leaving it ready to accept almost any prompt.

The most skilled attackers can take advantage of AI to save time, whether in more complex programming tasks or adjusting configuration files used in other tools.

Faced with these new challenges and the general outlook, there is a need to innovate in security. It is essential to harness advances that improve productivity and prioritize what matters most at the right time. Artificial intelligence and cyber threat intelligence are two important pillars of this effort.

It is not uncommon for cyber security to be impacted by external economic and political factors.

A good example is the popularity of cryptocurrencies and their regulation – or lack thereof. In practice, most ransomware attacks rely on payment in cryptocurrencies. It is a case in which a movement linked to economic policies ended up shaping a cyber coup.

In 2023, three geopolitical phenomena caused visible impact on information security: the war between Russia and Ukraine, trade sanctions imposed by the United States on China and, more recently, the conflict between Israel and Hamas.

Russia vs. Ukraine

- Movements in Russia impact criminals located in the country

- Authorities observing the conflict are seeing the need to create measures to reduce the cyber risk of critical sectors

- Economic sanctions make it difficult for third parties with connections to both countries to establish relations

When Russia invaded Ukrainian territory in 2022, starting the biggest armed confrontation on European soil since World War II, the war was soon mirrored on the internet. While campaigns recruited volunteers for the "IT ARMY of Ukraine", the Ukrainian government blamed the Russians for the denial-of-service attacks that left its websites unstable.

The Conti ransomware group was the protagonist of one of the most notorious episodes: after expressing its support for Russia during a major ransomware attack against the Costa Rican government, several conversations and information from the group were leaked. The exposure, attributed to a Ukrainian expert, is believed to have aggravated internal tensions and contributed to the dissolution of the gang.

- Ransomware-as-a-Service (RaaS) model
- Active since: December 2019
- Country of origin: Russia
- Most targeted sectors: large corporations and government agencies
- Motivation: financial

Of course, this did not happen to all groups that raised the Russian flag. The Stormous ransomware gang, which also declares itself pro-Russian, has continued to operate.

- Supposedly ransomware, but its mode of operation is being investigated
- Active since: 2021
- Most targeted sectors: governments, large companies
- Motivation: political agenda, financial gain

Several other attacks have hit critical systems in Ukraine and Russia since the start of the war. In June 2023, Ukrainians claimed responsibility for an attack that brought down an interbank network in Russia, creating instability in payment systems.

On the other side, a Russian group known as Sandworm has carried out several attacks against Ukrainian infrastructure. In November, attackers managed to destabilize the Ukrainian electricity system and cause a blackout that coincided with a physical attack. It was the third blackout caused by Sandworm, and the first that seemed to be linked to the Russian offensive.

- Threat group attributed to Russian military
- Active since: at least 2009
- Country of origin: Russia
- Most targeted sectors: electrical utility companies, government organizations, presidential campaigns
- Motivation: sabotage and espionage

But the repercussions of this conflict are not ☒ limited to both nations.

In 2022, there was no good explanation for the worldwide drop in ransomware activity. In 2023, the resumption of ransomware attacks ended up negating some explanations – such as the possibility that companies would simply be better protected.

Looking at what happened differently in 2022, we end up having to acknowledge the possibility that the drop in attacks was a possible consequence of the war.

It is widely known that many criminals involved in ransomware are Russian – or pro-Russia, as evidenced by Conti's actions against Costa Rica. At the beginning of 2022, Russia reorganized itself to adapt to the conflict, creating instability that may also impacted the routine of threat actors.

Internally, Russia was launching recruitment campaigns.

Externally, economic sanctions hampered the country's economic situation and access to the global banking system. Both are factors that may have hindered the criminals' activity.

The impacts are aggravated by hacktivist groups. One example is Killnet, which carries out distributed denial-of-service (DDoS) attacks and took down several websites in the United States and in European countries linked to the North Atlantic Treaty Organization (NATO). In early 2023, it began orchestrating attacks against health organizations.

- Pro-Russia hacktivist group
- Active since: 2021
- Country of origin: Russia
- Most targeted sectors: airports, banks, defense contractors, healthcare, internet service providers and governments
- Motivation: political, ideological reasons

In any case, it is clear that many nations have begun to review their national security plans.

Now that computerized systems are essential to the functioning of society, the role of technology and digital communication is part of this account.

As the conflict drags on and physical and cyber attacks are exchanged, more and more ideas and concerns are emerging – both in the digital and the business realms.

Economists have been saying that it is the end of the so-called peace dividend, a term popularized by President George H.W. Bush and Prime Minister Margaret Thatcher to describe the scenario that emerged after the fall of the Soviet Union, which allowed a reduction in defense spending. For many governments, it once again made sense to think of adversaries to justify measures.

The U.S Department of Defense's Cyber Strategy nominally mentions Russia and China as adversaries. The conflict with Ukraine is also mentioned as a demonstration of Russia's attack capabilities which, according to the White House documents, could target U.S infrastructure.

In practice, this means that the regulatory movements and economic incentives that the U.S government plans to develop are considering the reality of the conflict and that the new regulations that are coming to critical sectors – health, finance and infrastructure – can also be seen as an offshoot of the lessons of the conflict.

As many of the leading technology services and infrastructure providers are located in the United States, these changes will impact the entire world.

Another point to consider is the ↙ effects of economic sanctions and the business risks ⚠ associated with the supply chain that they impose.

Authorities have been imposing fines for violations – Microsoft itself was fined $3 million in April for having provided services irregularly.

This tension is fed from both sides. In addition to acting to isolate the country's network and reduce dependence on foreign software, Russia has fined three foreign companies – UPS, Airbnb and Spotify – on the grounds that they violated laws requiring data to be stored on Russian territory.

As technology service providers leave Russia to comply with legal obligations (including Microsoft, Atlassian and Amazon), companies that still rely on suppliers from that country may face risks to the availability, integrity or confidentiality of data under the responsibility of these third parties.

China and the semiconductor war

- → The U.S is seeking to expand its leadership in semiconductors, creating a geopolitical dispute with China

- → U.S argues that software and hardware made in China pose a national security risk

- → Countries have formulated plans to replace Chinese equipment

In 2022, the United States passed the CHIPS and Science Act. The legislation was a message that the country wanted to extend its technological lead over China.

The geopolitical relationships that made this necessary are complex. In addition to a possible relationship with problems in the global supply chain that arose during the COVID-19 pandemic, there are also military interests – for example, the United States has struggled to replace chips in old equipment.

In the face of reports that pirated chips from China have reached the U.S Military, it is understandable that the needs of national security and independence in semiconductor manufacturing have aligned.

In fact, U.S authorities have reiterated that the use of Chinese equipment creates risks to national security – both for the U.S and its allies. Security cameras made in China have been replaced and even banned in some countries, such as the U.K and Australia.

Something similar is happening in the dispute over 5G networks. Equipment from the brands Huawei, ZTE and Hikvision were banned in the United States at the end of 2022. Since then, some European countries have announced plans to replace Chinese equipment from their networks.

Even so, not all countries intend to adopt this type of measure, and it is unclear whether there will be any long-term consequences, especially for companies that do not operate on critical infrastructure.

Although the idea that discussion and negotiations should be based on facts and evidence is valid, the biggest fact is that this is a geopolitical dispute – which means that the interests involved are not always clear.

For this reason, companies that operate in critical infrastructure sectors or work frequently with the organizations affected should continue to monitor these developments, both from a compliance perspective and because of the concrete risks to connectivity and equipment security.

Israel vs. Hamas

- There are hacktivist groups on both sides of the conflict
- Hacktivists carry out symbolic attacks against organizations seen as allies of the adversary
- Although attacks are on a small scale, there is a risk of compliance and business damage
- The posture and response of organizations can be improved with Cyber Threat Intelligence

With the outbreak of the conflict between Israel and Hamas in October 2023, several hacktivist groups stepped in and declared their support for one side of the confrontation.

The mapping carried out by Axur's Cyber Threat Intelligence team identified

at least 52 hacktivist groups expressing support for Palestine, while 16 sided with Israel.

It is important to note that there are some links between this conflict and the clash between Russia and Ukraine. Some countries in the region – such as Iran and Syria – are Russian allies. This arrangement is reflected in the alignments of hacktivist groups as well, with the Ukrainian IT Army taking the Israeli side, while Killnet took the Palestinian side.

Just as in the Ukrainian case, these groups targeted their attacks at countries that expressed support for the opposing side, even when these countries were not directly involved in the conflict.

In this sense, we have cases such as the Ganosec Team, which attacked India for supporting Israel and to retaliate against Indian hacktivists who had spoken out in favor of the Jewish state. Moroccan Ghosts, meanwhile, targeted South Africa, claiming that the country supports Israel – even though historically South Africa is a supporter of Gaza, and joined the diplomatic embargo against the Israeli state.

Brazil, which submitted a proposal to the UN Security Council that classified Hamas' actions as terrorist, also attracted attacks from these hacktivist groups against local businesses.

Although Brazil has a very cautious stance towards the conflict and advocates a peaceful resolution, the mere condemnation of the attacks was enough.

The actions of hacktivist groups are not always directly related to their stated objective. This ends up representing a risk for several organizations, companies and even individuals, who may end up being caught in the crossfire.

Even small companies can be → attacked if these groups find a vulnerability that is easy to exploit.

The purpose of these groups' attacks is usually quite symbolic – the important thing is to demonstrate that they attacked a target perceived as an enemy. As long as the company or organization is linked to the hacktivists' target, any kind of attack – be it a DDoS or a data leak – is enough to prove commitment to the cause.

While many attacks aim to take down websites to share a screenshot of the "website down" error on communication networks (mainly Telegram), there are also cases where individuals' data is exposed and websites are defaced.

Data leaks create risks for people – as cybercriminals can also leverage this information for other purposes. However, there is also a compliance risk for any company that has a legal obligation to keep data secure.

Defacement incidents can be just as complex. Even though many hacktivists have no interest in causing other types of damage, the organization under attack still needs to carry out an incident response and forensics process that ensures the integrity of its environment. In addition, defacement actually has the potential to create embarrassment for the institution or brand, which is in line with the goal of these groups.

Applying Cyber Threat Intelligence can help speed up this response process, as groups often have a "signature" and their attacks tend to resemble their previous actions.

In any case, the variety of attacks and the difficulty of predicting the actions of hacktivists generate great uncertainty, and it is important to emphasize that no one is "off-limits" from being attacked. There are groups operating on both sides, and they attack any organization perceived as an ally or supporter of opponents – even if they have not declared being in favor or against the protagonists of the conflict.

↪ Although hacktivists are not always able to cause prolonged damage to national networks, a company that is unprepared to deal with these attacks can end up being exposed to several risks ⚠, as well as exposing its customers and employees.

2023 in numbers

2023 in
numbers

The Axur platform is always using data collectors and sensors configured to detect incidents from various categories, including credential leaks, card leaks, phishing pages and fraud such as brand misuse, fake social media profiles and fake mobile apps.

The year 2023 repeated a lot of what we observed in 2022. However, the form of leaks has changed significantly, and

↳ the number of leaked cards has more than tripled.

Credentials

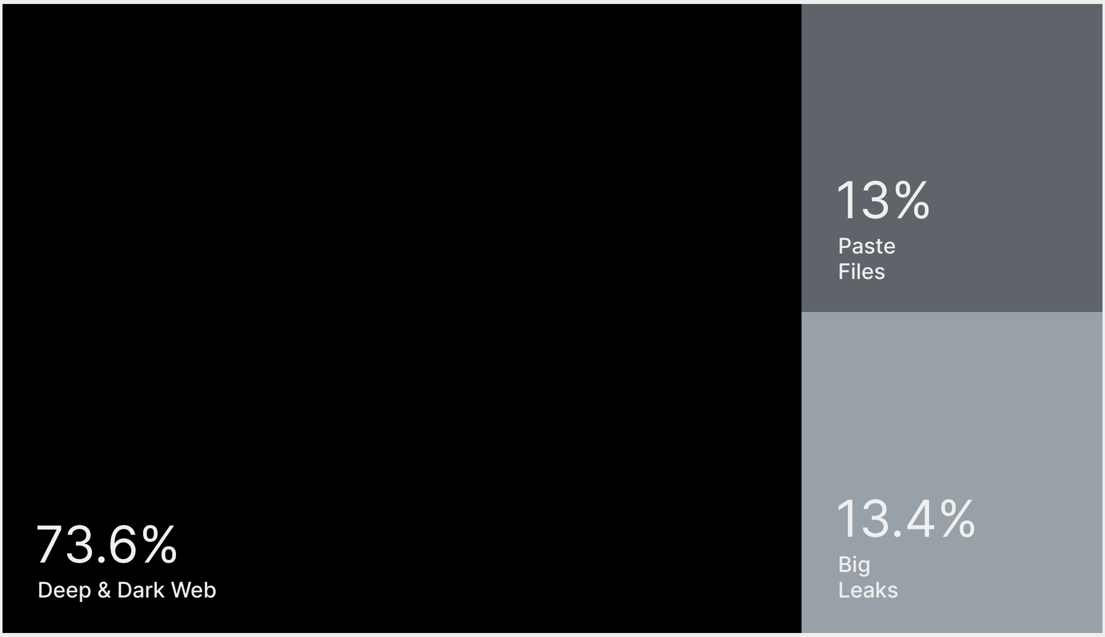
The Axur platform monitors leaks and posts on the Deep, Dark & Surface Web to identify leaked credentials.

In 2023, we detected the leak of 4.2 billion credentials, a figure that remained stable compared to the previous period.

Many credentials are extracted from systems attacked by credential stealing malware. These malicious software collects any type of credentials - they are capable of scanning browser data to steal cookies and searching for installed digital wallet software to steal cryptographic keys that give access to crypto assets.

Although the volume of leaked credentials has remained stable, there has been a change in the source of these credentials. In 2022, 96% of credentials were collected on the Deep Web. In 2023, we saw a much more significant number of credentials in so-called pastes and major leaks, increasing the diversity of credential sources.

Source of credentials in 2023



Deep & Dark Web channels, groups and forums continued to be the main sources of leaked credentials in 2023.

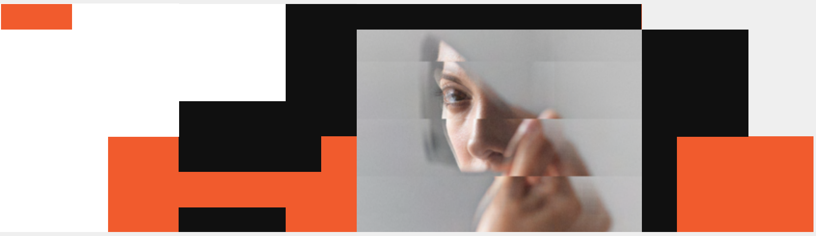
What is it?

Pastes: These are text files of varying sizes with often undefined complilations of data. The term is a reference to the text file format that can be shared on so-called paste sites.

Major leaks: Named or more specifically sourced data compilations are treated by Axur as a major leak. In general, these are voluminous databases that can be attributed to a source (a leak from a company) or to criminal action (a recompilation of smaller leaks).

Axur's analysis indicated that about 15% of credentials can be considered corporate.

However, this analysis is rarely easy to perform – many of the leaked passwords give access to accounts of popular services. Although these services are largely used for personal purposes, there are also cases where corporate data may be present in these accounts.



What sets stealers apart

It is clear that passwords should never be stored without some form of protection. Thanks to this, many credentials obtained from database leaks cannot be used immediately by criminals, making it necessary to break the encryption or hash of the stored password. Depending on the strength of the security, this may only be possible in the long term, when accounts have already lost their value or had their passwords changed.

In the case of credential stealing malware, this problem is practically non-existent. 98% of the credentials extracted by credential stealers were in clear text, that is, ready to be used in criminal activities.

Passwords obtained by stealers are disseminated in log files generated by malware. Criminals who are interested in a victim's log can acquire this data and know exactly how the credential was collected (from an app, a password manager or a browser, for example).

In addition to passwords, sтealeгs capture authorization тωкэns and cωωkies, which can bypass multi-factoг authentication (MFA/2FA).

These access tokens are generated after the user passes all authentication factors to ensure that the session remains authenticated from one access to the next – in other words, they are trusted by the authentication system. The attacker can insert the token into their software (either an app or the cookie in the browser) to clone the previously authenticated session.

The log also contains information about the computer, which may indicate whether the victim was an employee of a company or accessed corporate network services such as an outsourced provider.

Due to the risk posed by stealers, it is essential for companies to know if their credentials have been stolen and to invalidate both user's passwords and authenticated sessions after an attack.

The credential stealer can infect the victim's computer in a variety of ways and follows the Trojan formula. They can be spread through malicious web pages, social media posts, phishing emails or even fraudulent advertising. The software is offered as a useful program to the victim, who downloads it without suspecting that their credentials will be stolen.

Credential source

- Applications
- Password managers
- Browsers

Log

- Victim information
- Computer information
- Data on the corporation in which the victim works, either as an employee or as a contractor

How they spread the Trojan Horse

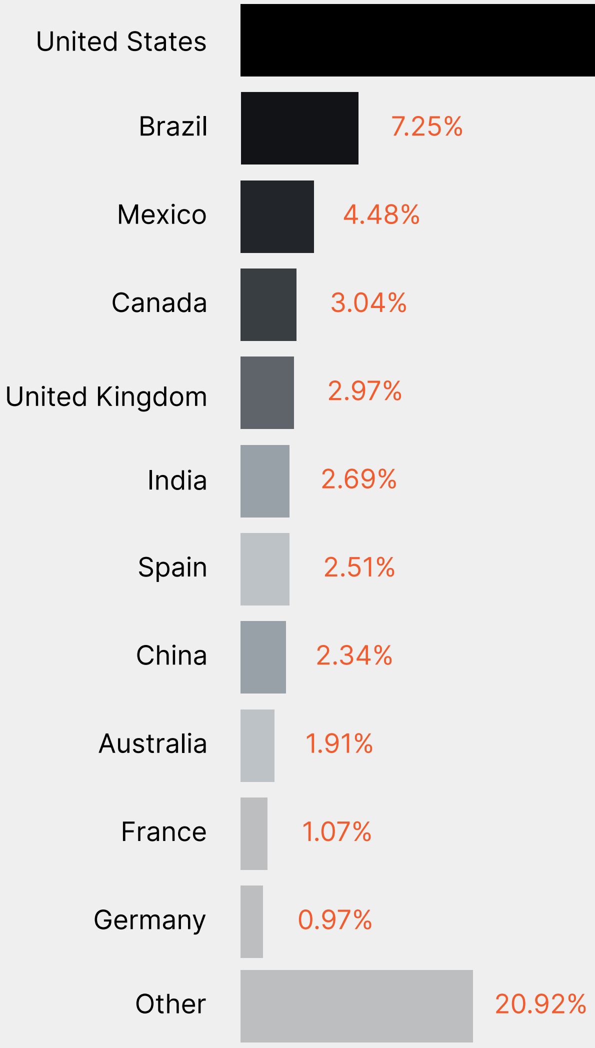
- Malicious pages
- Social media posts
- Phishing emails
- Fraudulent advertising
- Disguised as a useful software

Cards

The number of leaked credit and debit cards more than tripled in 2023 in Axur's detections: 13.5 million cards were leaked in 2023, an increase of 265% compared to the 3.7 million detected in 2022.

Approximately 83% of the cards were valid at the time of collection. In other words, the increase in the volume of cards compiled cannot be explained by an increase in the collection of expired cards.

Top 10 countries with the most exposed cards



First place in the ranking goes to the United States, with almost half of all detections.

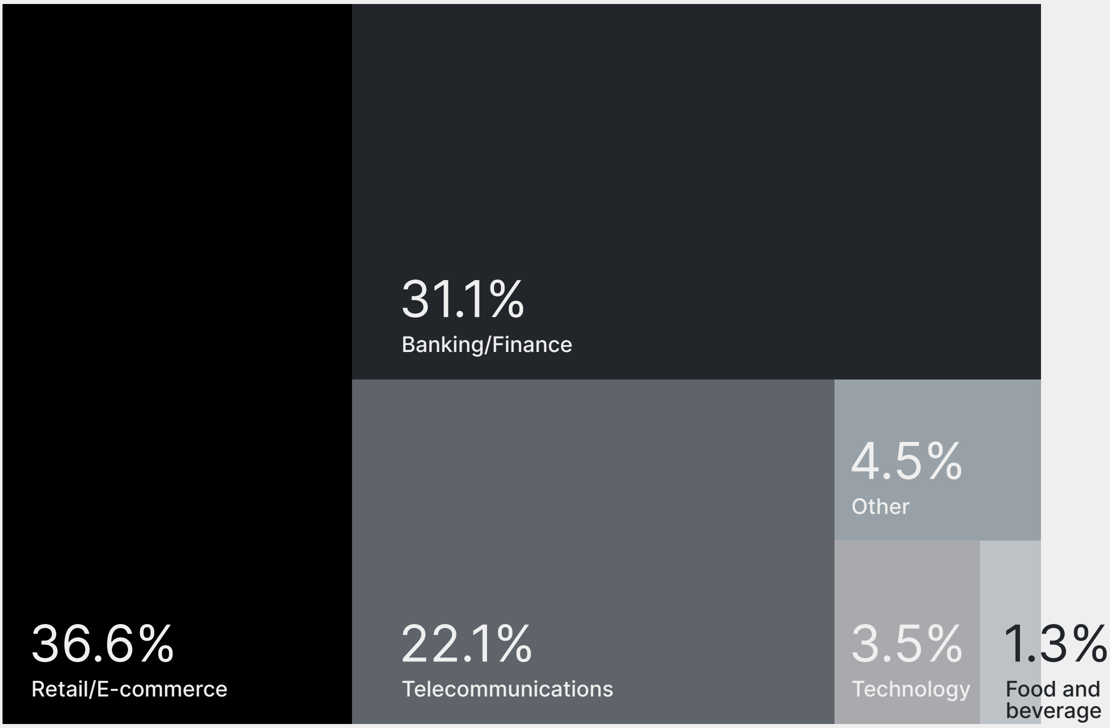
Phishing

Axur detects and counts phishing pages – that is, fake websites that steal user information (including passwords) or try to distribute malicious programs.

We detected 31,926 phishing pages in 2023, which represents an 8% drop from the previous year.

The most targeted sector was retail/e-commerce, which concentrated 36% of phishing pages. In second place were the pages of financial institutions and, in third place, telecommunication companies.

Top sectors targeted by phishing attacks

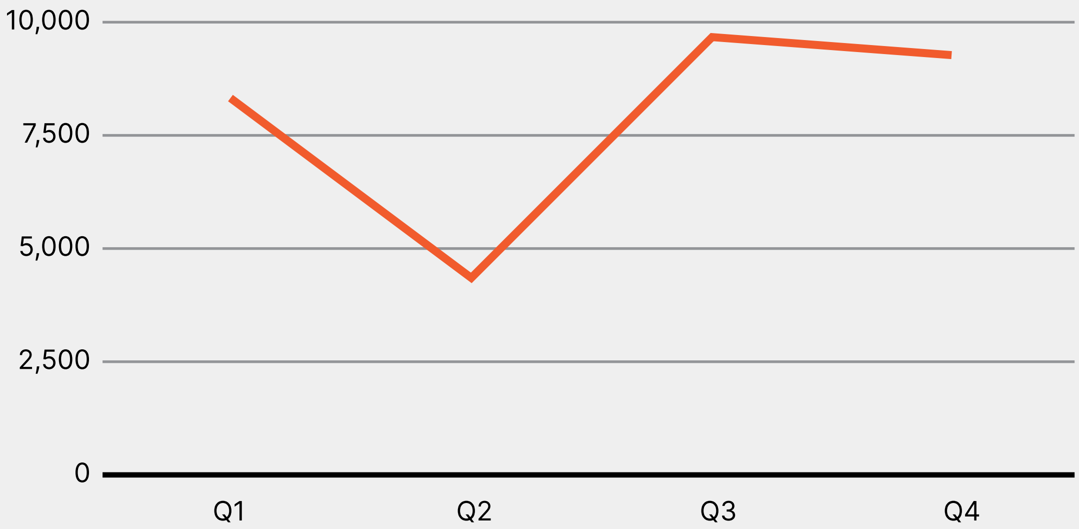


Three sectors concentrated about 90% of all phishing cases recorded in 2023.

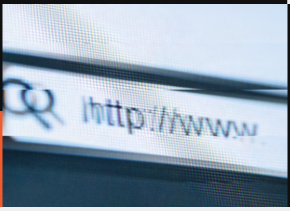
Phishing activity tends to be more intense from the third quarter onwards. Considering that retail is one of the most targeted sectors, criminals also carry out scams following the retailers' calendar – in other words, they tend to be more aggressive during end-of-year promotions and events, such as Black Friday and Christmas.

Unlike in 2023, the highlight was the third quarter, which registered the highest number of incidents. The last few months of the year maintained the increase, but without significant peaks.

Phishing cases per quarter



2023 numbers show an upward trend from the third quarter until the end of the year.



Use of Top-Level Domains

Just like any website, a phishing page needs an address to be accessed by victims. In this sense, we can look at the data to discover the habits and preferences of criminals when choosing the Top-Level Domains used.

A Top-Level Domain (TLD) is the suffix added to the registered domain to make a website available. ".com," ".com.br," ".org" and ".net" are examples.

For criminals, the choice of domain follows certain criteria:

→ The probability of misleading the user as to the legitimacy of the page:
If the ".com" version of a domain is already registered, the criminal may be able to register an address with the same name under some other suffix. Each TLD is a separate registry, which provides multiple opportunities for the malicious agent. A notorious example of this is ".co," which belongs to Colombia but is open to the whole world, being easily confused with a ".com" address.

→ The cost:
Some suffixes are cheaper than others.

→ The difficulty of taking down the domain:
There are registrars that do not tolerate the registration of websites with suspicious data or for improper purposes, which can prevent malicious agents from keeping their pages online. Criminals tend to prefer a more lenient register, with fewer rules.

Since 2012, ICANN – which coordinates authorization for new TLDs – has allowed any organization to propose a new domain (for a fee) and manage it if the proposal is approved.

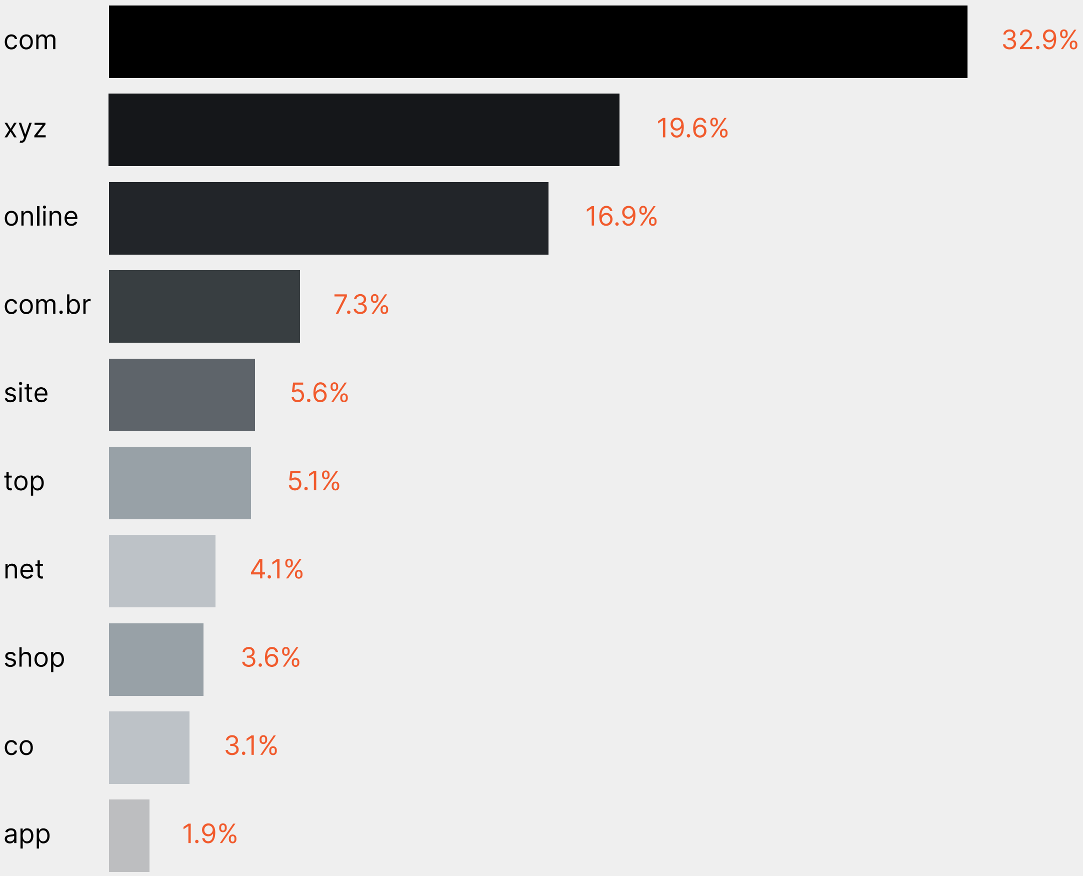
For this reason, there are currently more than 1,500 TLDs available and dozens of new suffixes awaiting approval. Each TLD that makes registrations available without restriction creates an opportunity for scammers to register addresses similar to those of the companies they intend to attack.

The pages observed by Axur tend to be hosted on popular addresses, such as those ending with ".com".

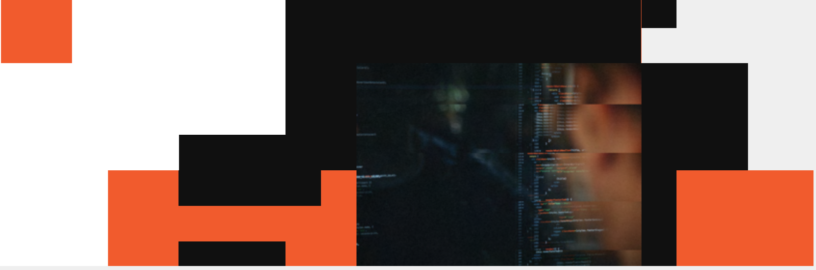
However, there has been a significant increase in the use of ".xyz" TLD in 2023.

The ".xyz" TLD was created in 2014 under the new ICANN rules. Registering these domains tends to be significantly cheaper, which may help explain the popularity of these addresses.

Most commonly used TLDs for phishing in 2023



The ".com" and ".com.br" TLDs are often used. But domains such as ".xyz" were the highlight of the year.



Deep & Dark Web

Monitoring the activity of criminal groups in environments outside the traditional web makes it possible to detect ongoing campaigns, gather intelligence on the tactics and procedures of malicious agents and even prevent incidents by prioritizing effective defensive measures in mitigating attacks that are being planned or discussed by criminals.

Filtering the material is a key part of this process. Axur's monitoring generates highly relevant alerts thanks to the combination of the advanced technology available on our platform with the configuration parameters customized by each customer.

To achieve complete visibility of criminal actions, we monitor messaging apps such as Telegram, WhatsApp and Discord, Deep Web forums and so-called markets – websites that function as e-commerce marketplaces for criminals. In these spaces, attackers offer leaked data, access to compromised computers, services and software for sale.

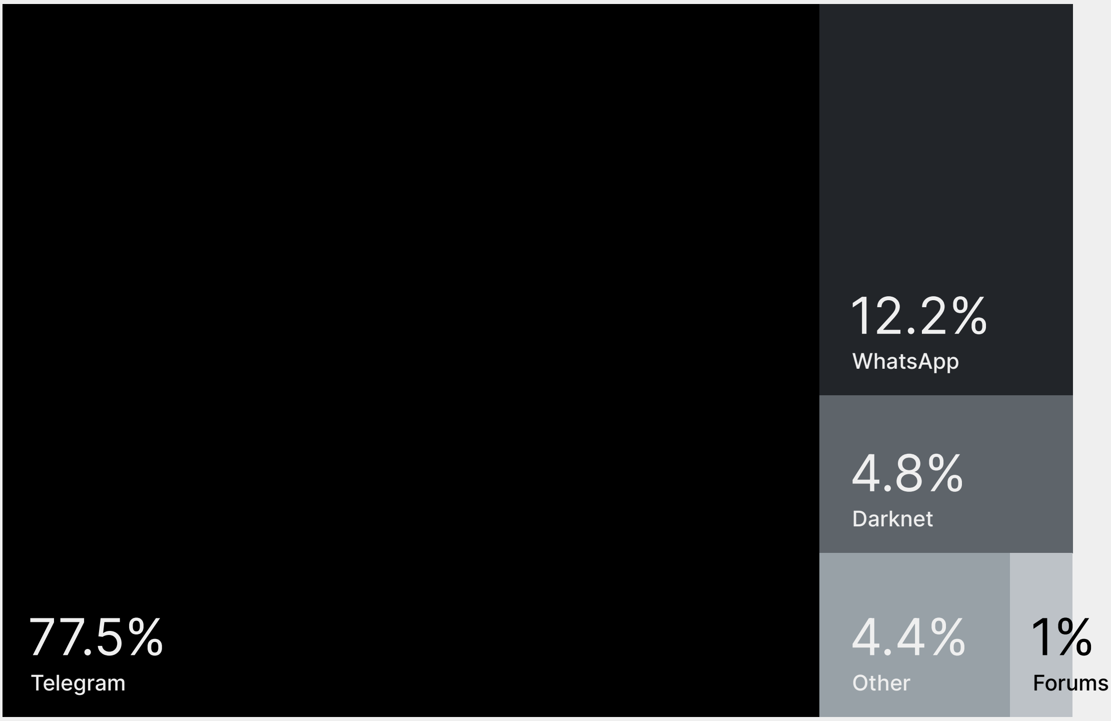
⚠

133 million

messages analyzed on the Deep & Dark Web

Axur's Cyber Threat Intelligence team also tracks interactions in these environments so that monitoring includes keywords commonly associated with attacks, incidents or fraud. This monitoring complements the detection of pastes and other leaks exposed on the Surface Web.

Source of Deep & Dark Web detections

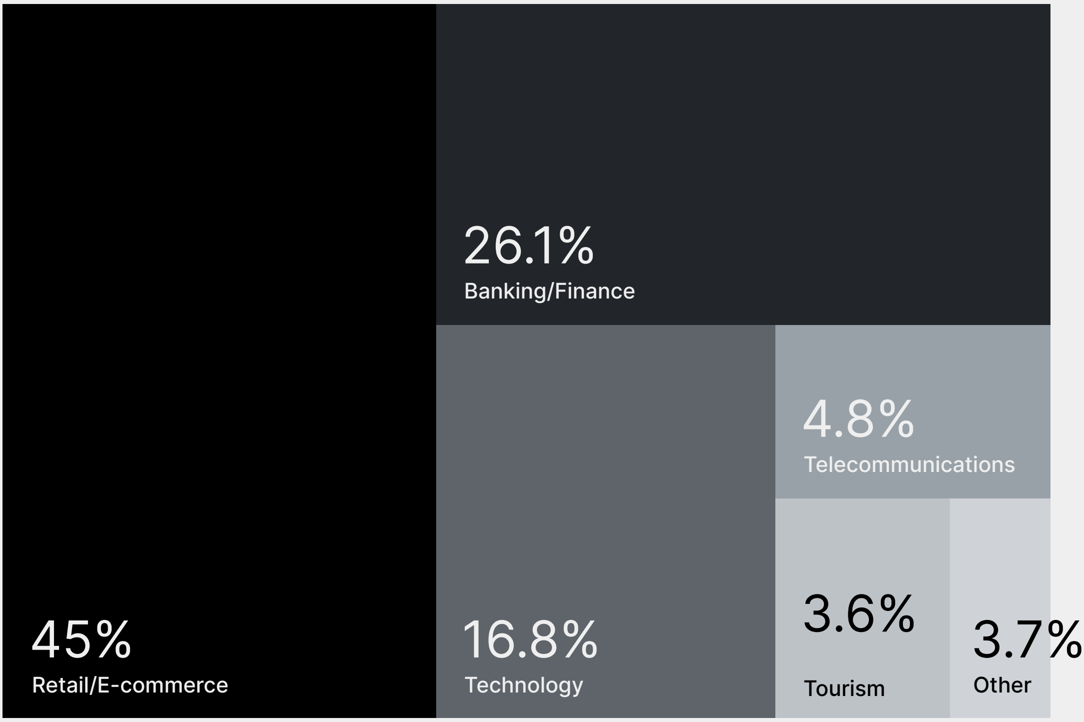


Detections amounted to 529,965 incidents on monitored Deep & Dark Web sources

As with phishing, the majority of suspicious mentions on the Deep & Dark Web were associated with companies in the retail/e-commerce, financial institutions and technology services industries.

It is important to consider that these mentions, although they indicate that certain companies are more targeted or numerically more attacked, do not mean that other sectors are ignored by criminals.

Most targeted industries on the Deep & Dark Web



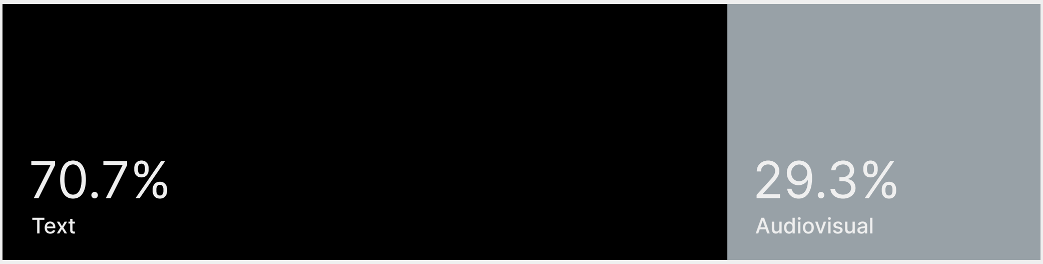
The year's detections concentrates the 3 most targeted industries

In-depth audio and video analysis

The Axur Platform uses artificial intelligence technology with deep learning to analyze content in images, audio and video. This way, even if the attackers use brand images accompanied by audio content, the platform is able to identify suspicious elements and create an alert according to the established settings.

In 2023, more than 1/4 of all alerts ⚠ generαted came from αudiovisuαl content analysis.

Artifacts that became alerts



On the Deep & Dark Web, 374,592 incidents came from text detections and 155,373 from audio, video or image detections

Analyzing images, audio and video tends to be more difficult and laborious, and would traditionally require an analyst to manually check this material. With a deep AI analysis, the search for links without analyzing this material, companies lose visibility into suspicious mentions of their brands or assets.

Exposed infrastructure

A company's technology infrastructure needs to be adequately protected to prevent attackers from finding loopholes that enable initial access to the corporate network. Even if an entry point does not seem particularly interesting, an attacker can apply lateral movement techniques to broaden access and reach more relevant systems, including domain controllers, databases and internal application servers.

Operational technology and Internet of Things (OT/IoT) devices deserve special attention. Security cameras, network equipment, or specialized and industrial machinery (including medical equipment) are some examples of this type of device. Businesses can be at risk when these devices are connected to the corporate network without proper registration of their presence or security procedures (for firmware updates, for example).

It is even recommended to use behavioral monitoring 👁 on these devices to detect non-standard activities, especially when traditional security solutions would not ☒ be effective in protecting the equipment.

Any exposure of these devices to the internet can represent an imminent risk of attack, especially since some legacy assets no longer have adequate support from manufacturers and cannot be replaced easily.

Another phenomenon that deserves attention is shadow IT. Employees can easily register corporate information in services that have not been cataloged by the IT department, or even use cloud computing resources irregularly, connecting internal and external devices without proper adherence to security processes.

Axur monitors data from infrastructure exposure to let our customers know about these and other risks arising from their technology infrastructure. Together with the detection of database exposure through the monitoring of Tracking Tokens, Axur's solution detects security policy violations in the most diverse scenarios.

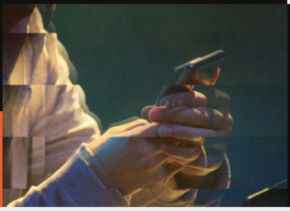
⚠

138.718

exposed infrastructure alerts

Because they are linked to the IP addresses used by the company, these alerts notify the security team about the existence of unknown exposed equipment that was not even known about.

Therefore, in addition to assisting in the regular application of patches to vulnerable systems, this work has the potential to prevent incidents involving security policy violations, shadow IT cases, and accidental OT/IoT connections to the external network.



Fake apps and fake accounts on social media

Criminals often take advantage of a well-known brand trusted by consumers to distribute malicious applications or make contact on social networks via a fake profile. In this context, the brand supports fraud and allows consumers to be reached directly.

In addition to harming the consumer, the brand itself can suffer damage to its reputation when this type of activity is not prevented through continuous monitoring. When a malicious agent realizes that it is more difficult to carry out scams using one brand, it tends to look for another, more vulnerable brand.

In the context of fake mobile apps, we have detected the growth of "apphishing" scams. These apps skip the functions that steal passwords or create overlapping screens that exist in most fake apps and instead load a cloned page controlled by the criminals. As such, the app itself is technically a web browser.

Since the information is fully captured in a system controlled by the criminal, app store filters do not always exclude these apps. In fact, it can be quite difficult to request the removal of these apps from stores, since the only evidence of malicious behavior is the misuse of a well-known brand.

Just like last year, we have a significant volume of fake profiles on social media and fake mobile apps.

Considering these categories alone, there were 116,445 detections of 📱 fake profiles and 18,712 fraudulent apps.

Other misuse of the brand

In addition to appearing in profiles and apps, brands can be mentioned without authorization in several other contexts, misleading consumers and linking the company to products, services, or promotions that cannot be validated by the company.

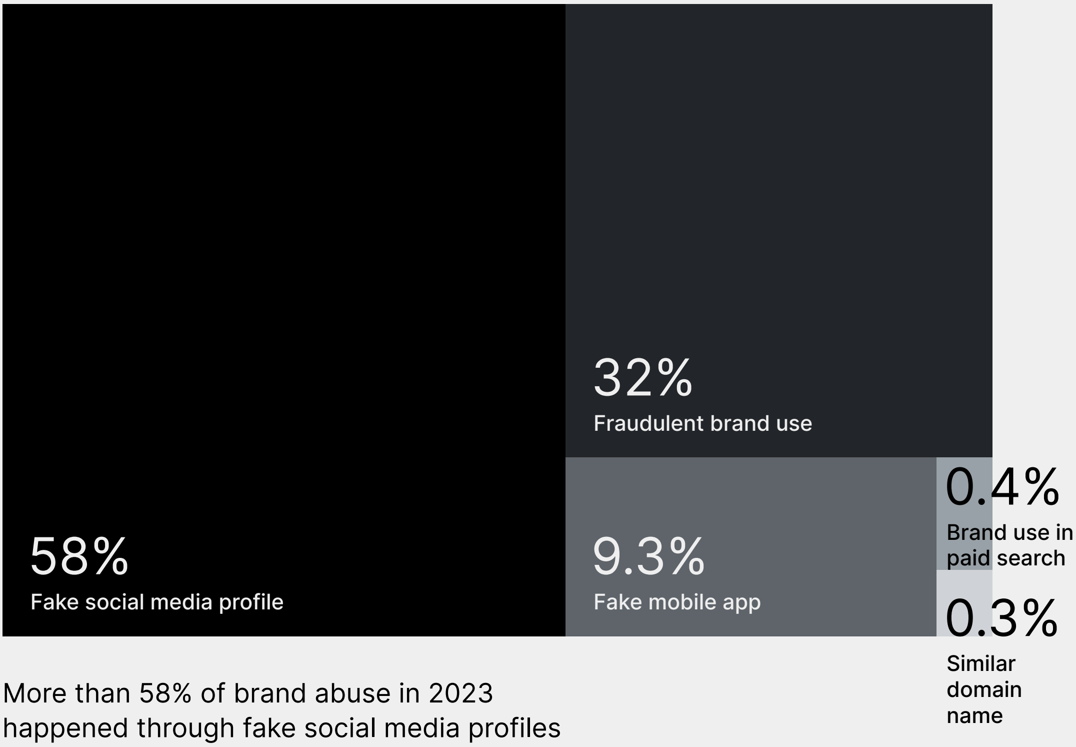
There are even situations in which criminals pay for advertisements using the brand without authorization to lead the victim to offers without any legitimacy. In the most severe cases, advertising can spread a phishing page or malware.

Thanks to platforms that allow you to create e-commerce stores in minutes, scammers have also been creating entire stores under the names of well-known retailers. As these platforms offer their own payment channels to make it easier to set up a store, criminals take advantage of these payment intermediaries to hide where the money is going.

Adding these other cases
of unauthorized use, we had

200,680 detections in 2023, a stable volume compared to the number of 193,000 detections in 2022.

Types of brand abuse



More than 58% of brand abuse in 2023 happened through fake social media profiles

Boosting the response: Axur's Takedown numbers

Given this scenario, the response to digital fraud cases needs to have differentials to reduce the fraud exposure time and mitigate impacts for the consumer and the brand.

In 2023, we performed 330,612 takedowns ↓ maintaining a high success rate, including for threats such as pнisнiпg (96.85%) and ʄɑke profiles (97.63%).

Given that the analysis time of notified entities is beyond the control of those requesting the takedown, the main factor influencing the time to remove an incident is to rely on automated notification flows, reducing the window between identifying an incident and sending the notification to the platform or provider. Axur carefully designs these flows to address the right channels with the right message. This approach not only ensures that notifications are sent efficiently but also that they are highly effective, resulting in impressive uptime figures (time until the reported fraud is removed by the responsible entity).

Phishing:

To combat phishing cases, the Axur platform notifies organizations within 5 minutes. Smart notification flows can trigger messages to two channels in a single record – for ISPs or providers.

The following chart shows the uptime in the organizations with the highest number of takedowns performed by Axur in 2023: Shopify, Cloudflare, Namecheap, Hostinger, and GoDaddy.

Notifications are usually processed on the same day.

Chart - Phishing removal uptime by organization

Organization	Uptime (hours)
shopify	9.69
CLOUDFLARE	13.74
namecheap	13.96
HOSTINGER	17.96
GoDaddy	27.21

Most phishing incidents end on the same day

Fake social profile

Axur's takedown processes achieve high efficiency even in situations with a high volume of notifications, such as on the world's largest and most used social networks.

On Facebook, after the platform's notification, we were able to remove these accounts in an average of just 41 minutes, while on Instagram the uptime is up to 56 minutes before the accounts are removed.

Uptime of fake account removals by platform

Organization	Average Uptime (m)	Average Uptime (h)	Average Uptime (d)
f	41.67	0.69	0.029
◎	56.14	0.94	0.039
♪	3,817.33	63.62	2.65
X	3,591.17	59.85	2.49

For most cases, removal time is even shorter, with removals executed in as little as 15 minutes

In addition to notifying the proper channels in the shortest time in the industry, uptime is also impacted by changes and trends from the responsible entities themselves.

In the context of social media accounts, it is worth highlighting the changes that have been taking place on Twitter – now called X. Following Elon Musk's acquisition of the platform, the social network laid off employees (including reducing the team responsible for content moderation) and changed policies to lessen the perception of censorship.

Due to the changes, Axur observed a difficulty in handling incidents of fake accounts on X. Although it is still possible to take down profiles that improperly exploit brands, the notification response time (uptime) of these accounts was impaired for a long time throughout this year, until the Axur team was able to resume automatic notification flows.

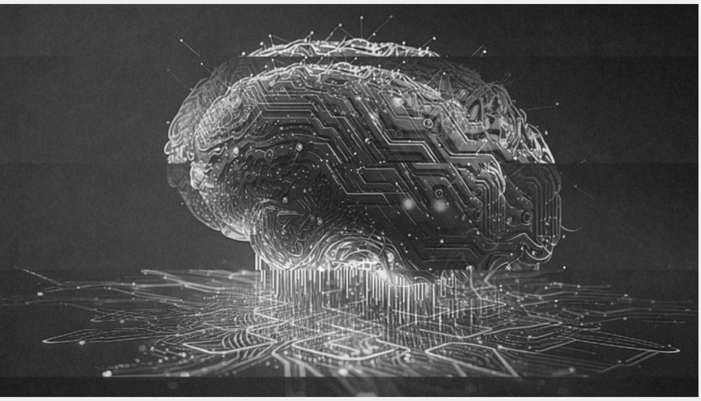
These flows again came into jeopardy with another worrying development announced by X in December. The announcement that the platform is planning to require facial recognition for fake profile notifications could directly impact the takedown process of fake profiles of Executives and VIPs - sensitive accounts often targeted by cybercriminals.

Axur continues to closely follow the developments of X's new policies to implement new solutions for monitoring and reacting to the risks hosted in Musk's territory.

Trends

Looking at the threats that stood out in 2023 and the strategies that worked – for both attack and defense – we can get an idea of what could come next and mark the year of 2024.

Artificial Intelligence



Artificial intelligence technologies, especially the new types of generative AIs, have generated new opportunities and working methods. The same movement is already happening in cybersecurity.

The use of large language models, such as chatGPT or Bard, enables criminals to devise customized but large-scale scams, such as spear phishing attacks in which the AI automatically adapts to the context and type of language of each victim. In broader actions, such as traditional phishing, there is an expectation that AI will begin to personalize the message for each recipient, bringing features that would normally only be seen in targeted attacks.

Generative AIs that manipulate images open up a particularly wide range of possibilities, whether it's the creation of images dedicated to each recipient or fake extortion scams. A common theme in these scams is the threat of exposing sensitive images of the victim in explicit or nude scenes. In general, criminals are unable to provide the images in question – after all, it's a fake threat – but AI can change that.

There have already been cases where individuals have misused AI to create fake nude images of other people. What remains is for this to become an element of everyday cyber attacks, either in the form of fraud or as part of a social engineering approach.

The threat of generative AI to authentication systems could also get ⚠ worse.

The improvement of AIs capable of generating movements or spoofing voices could push existing remote authentication systems to the limit, requiring them to be adapted or even rethought. The risk of this activity is not limited to companies, as e-government processes are equally dependent on robust authentication.

On the defensive side, there is a great opportunity for the use of artificial intelligence in the context of Cyber Threat Intelligence. AI makes it possible to associate and prioritize threat information taking into account the attack surface of each organization, quickly establishing relationships between large volumes of data. In the generative stage, this prioritized and highly relevant analysis can be presented in such a way as to guide practical actions to prevent or deal with incidents.

Although AI has its limitations, in general its agility can fill a gap that would hardly be feasible for humans. It is, therefore, a new way of obtaining intelligence, with tools that provide a good level of accuracy in the results.

The U.S government has already announced that it intends to look for ways to integrate ↔ artificial intelligence into the protection of critical infrastructure, including to find vulnerabilities in its systems.

At the same time, this initiative must propose countermeasures to prevent AI from being misused.

It is worth noting that other Deep Learning modalities have already been applied to alert screening and the recognition of behaviors and patterns to detect threats.

Gateways:
social engineering and supply chain

Social engineering is a constant element in the early stages of an intrusion, although it is not always the attacker's only tool (there can be a combination of social engineering and zero-day breaches, for example). A more recent development, however, is the focus on attacking third parties – businesses or individuals associated with the target, but who are not included in the environment protected by traditional security measures.

Social engineering is a major factor in this context, since training and awareness initiatives are not always homogeneous between a company and its suppliers. The gap in the preparation and prevention of attacks can create an entry point for the attacker.

It's worth noting that attacking these partners also opens up new avenues for social engineering. The attacker can obtain information through these third parties or use a provider's systems to deceive their real victim. This happened with MailChimp in 2022, which was attacked – via social engineering – for providing services to crypto-asset companies, but the activity intensified and diversified in 2023, with attacks on other industries. In the Caesars Entertainment and MGM Resorts incidents, the attackers used social engineering against an external IT service provider.

For advocates, it is important to understand that the adoption of cloud computing or software-as-a-service (SaaS) systems cannot be seen as a way of reducing risk. Attacks against these third-party systems also generate risks for the company, and the service provider cannot be held liable for all the losses resulting from a breach or downtime.

Considering that these technologies can be used to gain productivity and reduce costs, it is understandable that companies will look to streamlining their ecosystems as a way of controlling risk and exposure to many environments.

In this context, it is necessary to find solutions capable of mitigating both internal and external risk and, at the same time, preventing the expansion of the attack surface and the complexity of the IT ecosystem.

The integration of different technologies and approaches into complete cybersecurity platforms reduces the costs of adopting and configuring solutions, as well as simplifying the relationship with suppliers.

Managed platforms are also more accessible to small and medium-sized companies that make up the supply chain of large corporations.

Physical threats

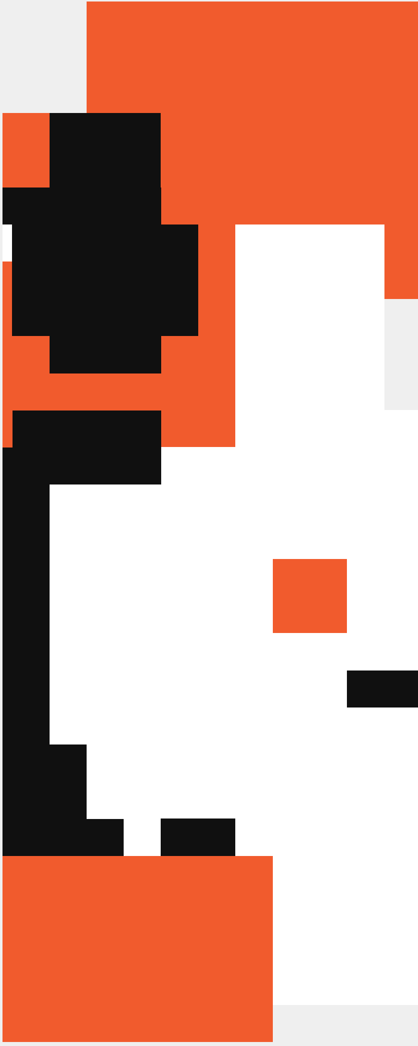
The barrier between what's real and the virtual in information security is no longer so clear. The blackouts in Ukraine are currently the most concrete example of the physical consequences of cyber attacks. And in the private sector, the healthcare sector is one where this issue is a major cause for concern.

In the same vein, social engineering scams are emerging that incorporate threats of physical violence. Attacks of this kind have been carried out by the "Scattered Spider" group, a group of actors who also attack third-party providers – which means that both techniques can appear together.

Attacks against physical security devices (including security cameras) can also have this kind of impact. However, these attacks have happened before and there seems to be no reason to expect any significant change in this scenario – unless new facts come to light.

This is not to say that these attacks are not a concern in infrastructure and health contexts. New regulations in the United States and Europe have been implemented to reinforce the safety of industrial and medical devices: the Food and Drug Administration (FDA) now obliges manufacturers to document measures that guarantee the safety of medical devices.

Consumers and small businesses can also expect some improvement. The European Union has a comprehensive Internet of Things (IoT) policy and, if successful, this stance could make some attacks more difficult – at least on devices that comply with the rules. The U.S Federal Communications Commission (FCC) has proposed a seal, or trust mark, to make consumers aware of the security of smart devices.



> On the other hand, it is undeniable that there are a large number of legacy systems still in use and it is not always easy to assess the risk they pose.

Because of the difficulty in assessing the risk, some of these devices have ended up in the crossfire of geopolitical tensions with China, where many of them are manufactured. Chinese-made cameras have been restricted in the United States, the United Kingdom and Australia. More recently, there has been a movement to restrict the purchase of drones – both by China, which has established export rules, and by some U.S authorities who fear the existence of insecure codes that lead to the exposure of data collected by these devices.

Elections and misinformation

The year 2024 is an election year for the United States. Because it's an election year, political priorities can change, either temporarily or permanently. Since the U.S plays a central role in world geopolitics, the country's actions and reactions can have a considerable impact on the course of events.

In practice, many threat actors linked to opposing countries – whether officially or through political affinity – will have some interest in the outcome of the election.

This translates into challenges for the U.S election itself. As in previous elections, it is possible that external agents will try to interfere in the election by

manipulating social media ⊟ posts or even cyber ατταcks against certain politicians.

It is possible that there will be some surprises due to the involvement of hacktivist groups. Although they don't usually have the same effectiveness as more coordinated agents, it can't be ☒ ruled out that they are involved in some revelation with a political impact.

These more coordinated agents can incorporate new technologies into misinformation campaigns. As much as social media platforms have learned to reinforce their monitoring efforts in previous elections, the use of deepfakes – convincing images and audio doctored AI – has the potential to wipe out much of the progress made in the fight against fake content.

In addition, the circulation of content through closed or private channels – on platforms such as Discord and Telegram – can make it difficult to identify this material. Temporary and short content – such as stories and short-form videos – are also more popular today than in previous elections, and the impact of fake content in this type of format can be more difficult to measure.

Strategies and tactics for 2024

Strategies and tactics for 2024

After exploring the emerging trends of 2024, it is clear that the risks are evolving rapidly. In response to this dynamic scenario, Axur has dedicated its development and data science team to exploring the potential of generative artificial intelligence throughout 2023.

The result is a revolutionary solution that we believe represents the next generation in Cyber Threat Intelligence. Now, at the start of 2024, we introduce this innovation in the field of defense: the new era of CTI.

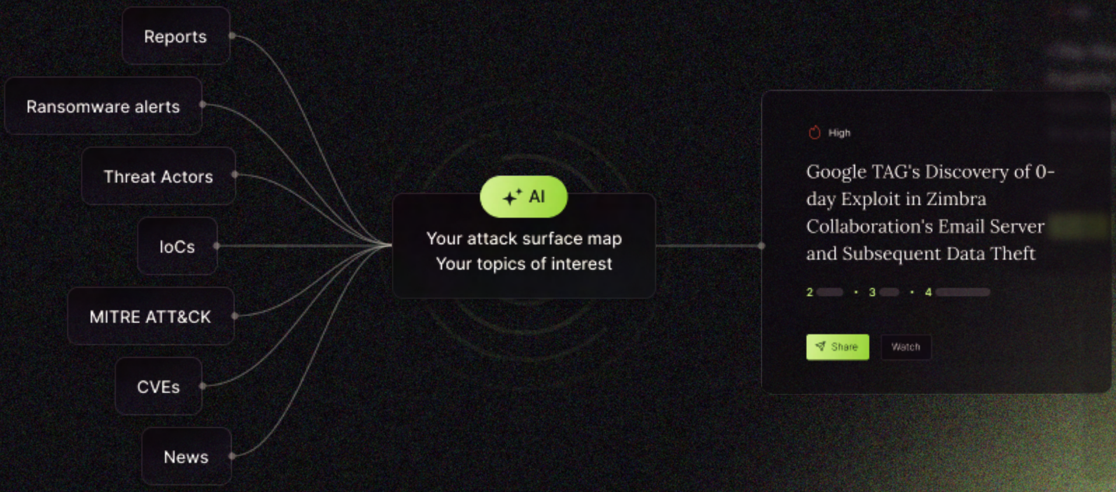
Polaris

Meet POLARIS, your AI-enhanced Threat Intel analyst

Axur presents Polaris, the solution designed to be the first in CTI where AI is not just a feature added to the product – it is the product itself. Imagine having an automated analyst at your side who operates 24×7 on your behalf, using LLMs with the most advanced technology to read, inspect, cross-check data and prioritize the most relevant threats every day.

How does Polaris work?

- Polaris takes stock of your attack surface (ASM) and your topics of interest, with advanced and unprecedented customization.
- Every day, it analyzes hundreds of sources, including news and information on common vulnerabilities, ransomware alerts, IoCs, frameworks (MITRE ATT&CK) and exposures (CVEs).
- Its highly specialized LLM model summarizes each relevant attack, threat or vulnerability.
- It then filters out everything that pertains to the map of your attack surface and the topics of interest you have selected.
- It generates curated, actionable alerts with only what you need to know, nothing more.



Your strategic analyst 180x faster
in identifying and screening threats

Insights acionáveis de cibersegurança, não apenas notícias

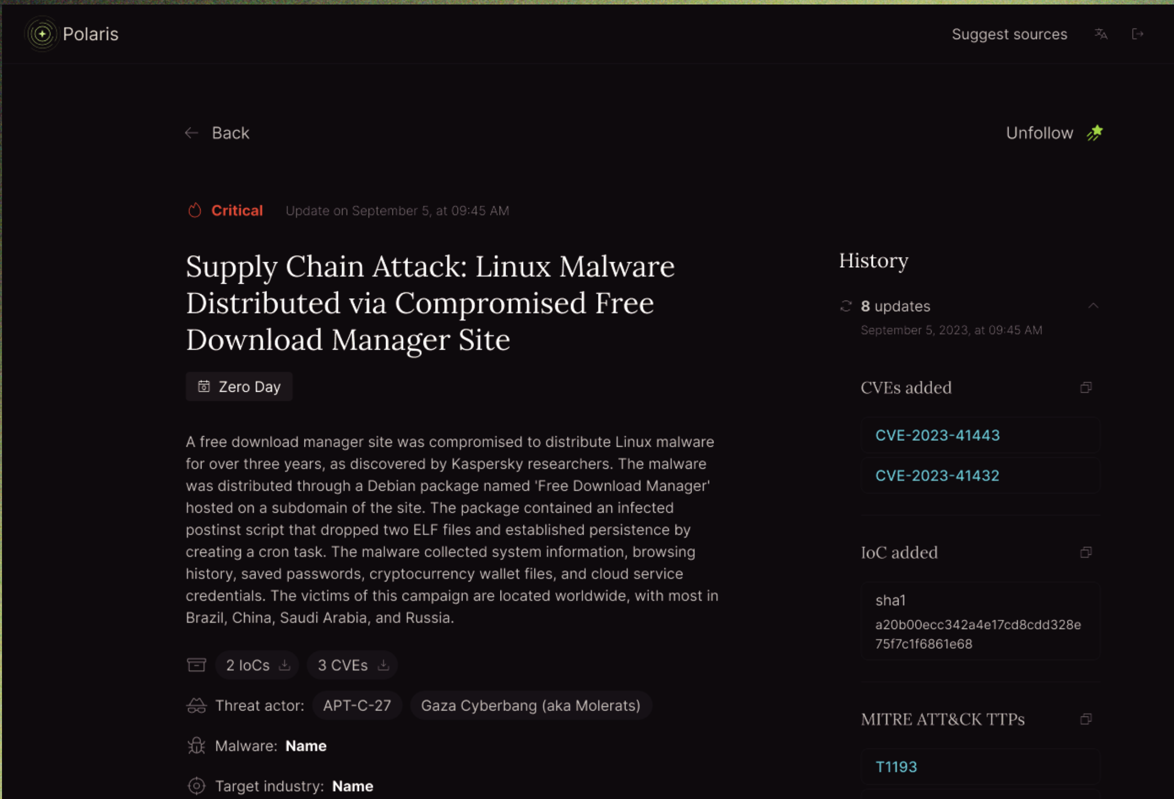
→ Filtered information: based on location, date, threat actors, motives, TTPs (Tactics, Techniques and Procedures), associated CVEs, affected sectors and protective measures.

→ Insights generated: personalized for you, explaining the importance of each point and what you can do to stay protected.

Free trial

And experience the power of an automated Threat Intel analyst

Go to: axur.com/polaris



Critical   Update on September 5, at 09:45 AM

Supply Chain Attack: Linux Malware Distributed via Compromised Free Download Manager Site

Zero Day

A free download manager site was compromised to distribute Linux malware for over three years, as discovered by Kaspersky researchers. The malware was distributed through a Debian package named 'Free Download Manager' hosted on a subdomain of the site. The package contained an infected postinst script that dropped two ELF files and established persistence by creating a cron task. The malware collected system information, browsing history, saved passwords, cryptocurrency wallet files, and cloud service credentials. The victims of this campaign are located worldwide, with most in Brazil, China, Saudi Arabia, and Russia.

2 IoCs   3 CVEs

Threat actor: APT-C-27   Gaza Cyberbang (aka Molerats)

Malware: **Name**

Target industry: **Name**

History

8 updates
September 5, 2023, at 09:45 AM

CVEs added

CVE-2023-41443

CVE-2023-41432

IoC added

sha1
a20b00ecc342a4e17cd8cdd328e75f7c1f6861e68

MITRE ATT&CK TTPs

T1193

///AXUR

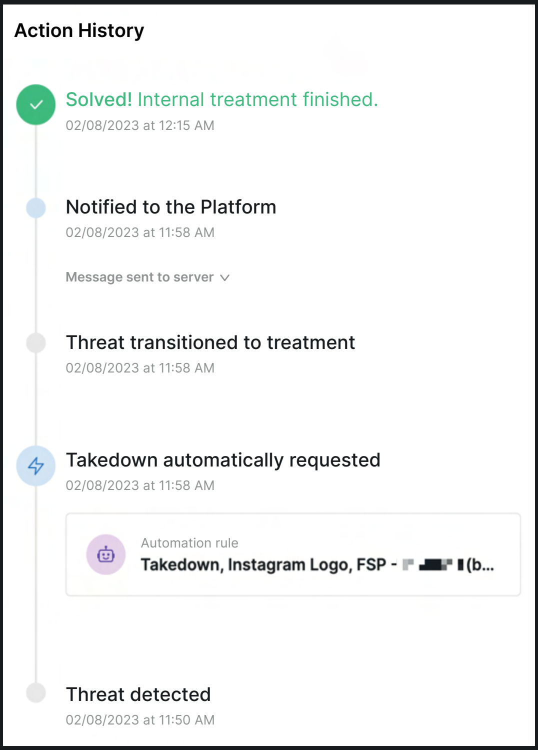
More on the Axur platform

End-to-end automation

Less noise, more relevance. Scale up the analysis of a massive amount of signals and the handling of relevant incidents through intelligent automations based on various attributes identified by AI..

Inspeção com IA

☑ Logo similarity
☑ Content language
☑ Brand name disambiguation
☑ Risk level
☑ Presence of password field
☑ Facial recognition of VIPs
... and much more!



Action History

Solved! Internal treatment finished.
02/08/2023 at 12:15 AM

Notified to the Platform
02/08/2023 at 11:58 AM
Message sent to server

Threat transitioned to treatment
02/08/2023 at 11:58 AM

Takedown automatically requested
02/08/2023 at 11:58 AM
Automation rule
Takedown, Instagram Logo, FSP - [redacted] (b...

Threat detected
02/08/2023 at 11:50 AM

Real example of results from a company in the financial sector

Automation rules

Set up automation flows to have an unbeatable arsenal working 24×7 for your business, identifying risks and requesting automatic takedowns. Sleep easy, knowing that whenever the conditions you determine are met, the threat will be dealt with immediately.

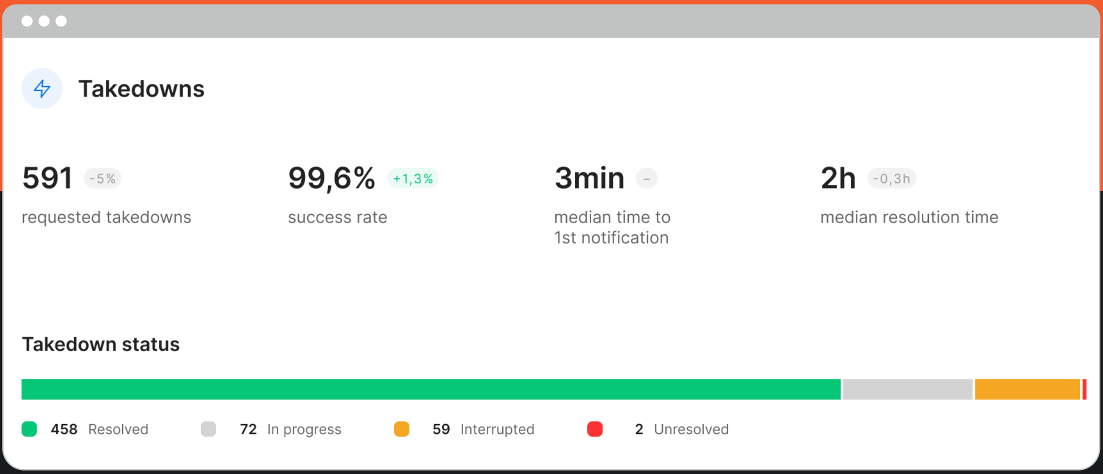
More than 86% of detections at Axur in 2023 were handled without any human touch.

The best Takedown in the world. And we can back it up:

5
minutes
For the first notification in phishing cases and up to 30 minutes for other cases

98.9%
success rate
With a guarantee of a new takedown if the content comes back online within 15 days

10h
uptime
Average record time for content removal with Axur takedowns



Takedowns

591 -5%
requested takedowns

99,6% +1,3%
success rate

3min –
median time to 1st notification

2h -0,3h
median resolution time

Takedown status

🟩 458 Resolved ⬜ 72 In progress 🟧 59 Interrupted 🟥 2 Unresolved

| Real example of results from a company in the retail and E-commerce sector over a period of 30 days

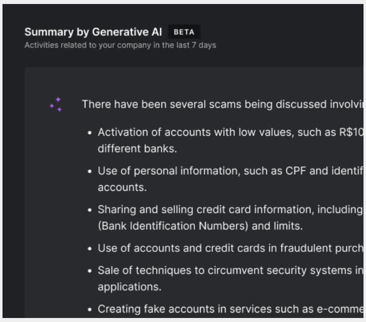
Takedown with automated flows, because you can't wait for human action when you most need agility to remedy the problem.

Drastically reduce mean time to containment (MTTC) by automating the part of the process that you can control with the fastest and most assertive notifications on the market. Optimize provider analysis with orchestrated notifications for the best route and message, developed with years of experience - and constantly improving. If the notified entity begins to show signs of a delayed response, new flows are automatically triggered to speed up the takedown by another route. All this makes it possible to scale takedowns in an unlimited way.

Intelligence that scales

The amount of noise and reliance on manual processes are already well-known problems for security teams. You need a Threat Intelligence platform that leverages the scale of analysis and action in your company's defense strategies.

Axur automatically collects and processes a vast volume of data, producing the most relevant insights through curation, normalization, enrichment and risk assessment. This way, you can prioritize your efforts quickly enough to reduce the attackers' window of opportunity.



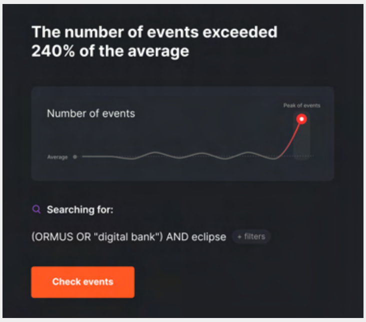
Summary by Generative AI BETA
Activities related to your company in the last 7 days

There have been several scams being discussed involvi

- Activation of accounts with low values, such as R$10 different banks.
- Use of personal information, such as CPF and identif accounts.
- Sharing and selling credit card information, including (Bank Identification Numbers) and limits.
- Use of accounts and credit cards in fraudulent purch
- Sale of techniques to circumvent security systems in applications.
- Creating fake accounts in services such as e-comme

DeepChat

You don't need to delve into all the events of the Deep & Dark Web to get an objective view of what's going on. Start your day with a briefing of the most relevant mentions of your brand with DeepChat, our own generative AI model fluent in the language of cybercrime. Get accurate insights to optimize your threat management and still have an executive report at hand whenever you need it.



The number of events exceeded 240% of the average

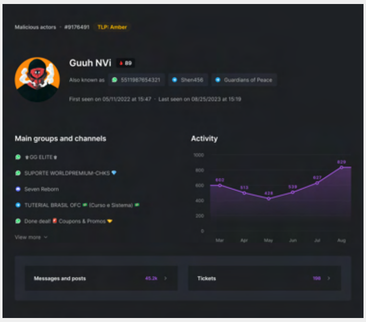
Searching for:

(ORMUS OR "digital bank") AND eclipse

Anomaly alerts

Set up alerts for anomalies such as higher than normal mentions, on specific channels or with keywords you choose. Whenever an anomaly is detected, an alert is sent to draw your attention in good time to what is most relevant. Act quickly and avoid surprises.

The alert warns you in real time, for example, if malicious actors are planning attacks or exploiting bugs in your business. This way, you can react more quickly without having to constantly monitor each detection.



Malicious actors · #9176491 TLP: Amber

Guuh NVi 89

Also known as 5511987654321 Shen456 Guardians of Peace

First seen on 05/11/2022 at 15:47 · Last seen on 08/25/2023 at 15:19

Main groups and channels

- GG ELITE
- SUPORTE WORLDPREMIUM-CHKS
- Seven Reborn
- TUTERIAL BRASIL OFC (Curso e Sistema)
- Done deal! Coupons & Promos

View more

Activity

Messages and posts 45.2k

Tickets 198

More threat intel features

AI-determined Threat Actor Profile and Score, CIs, ransomware attack alerts, threat reports and investigations from our team of experts are ready to sophisticate your intelligence capabilities.

A single platform to protect your business in the digital world

Digital fraud

Monitor and detect content impersonating your brand, with 24/7 coverage. Use the world's most efficient takedown to automatically remove external risk vectors.

- ☑ Phishing
- ☑ Fraudulent brand use
- ☑ Malware
- ☑ Fake social profiles
- ☑ Fake mobile app
- ☑ Similar domain name

Data leakage

Be alerted to improperly exposed data, reduce reaction time and reduce the attack surface on your business

- ☑ Infostealers credentials
- ☑ Credit card exposure for issuers
- ☑ Credit card exposure for applications
- ☑ Corporate credential exposure
- ☑ Sensitive Data
- ☑ Leaked code secret
- ☑ Database exposure

Deep & Dark Web intelligence

Use the largest integrated database of raw data from the Deep & Dark Web to monitor cybercrime activity, detect mentions of your business and stop attacks in the shortest reaction time.

☑ Mentions of your business, partners, industry or any keyword you want to monitor, including in images (using OCR) or audio, with transcription

☑ Indicators of Commitment (IoCs)

☑ Security bulletins

☑ Targeted searches and Threat Hunting with Explore

☑ Anomaly alerts

☑ Immediate support for research and investigation

Executives and VIPs

Monitor the data exposure of your company's most sensitive accounts and reduce the risk of spear phishing, ransomware and social engineering attacks.

☑ Fake social media accounts

☑ Exposure of personal information, credentials, telephone numbers or credit cards

Online Piracy

Get back your revenue that is being lost to piracy and illegal sales.

☑ Fake product or irregular sale

☑ Content piracy

Security assessment

Evaluate and strengthen your security posture by eliminating external and third-party risks

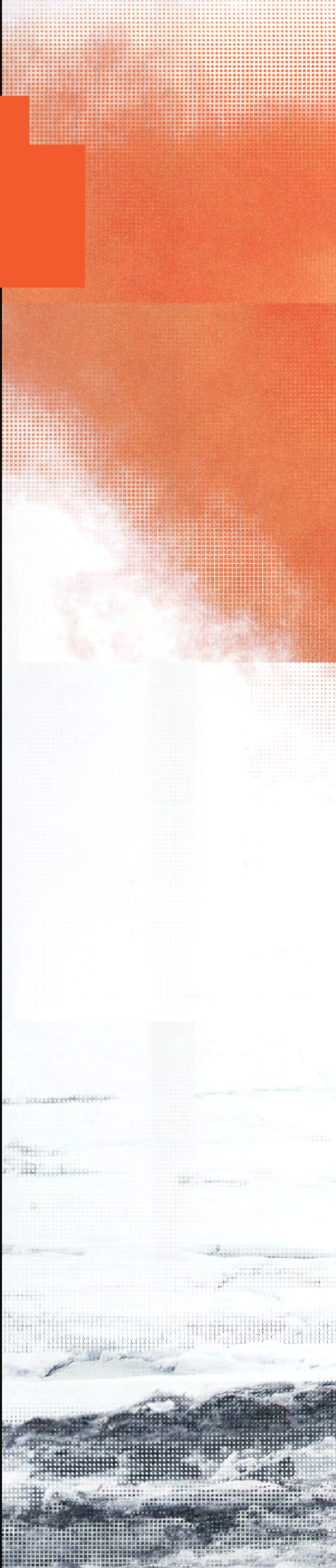
About AXUR

Axur enables the scaling and automation of cyber threat treatment to support information security teams and provide safer digital experiences. Our Threat Intelligence platform has the fastest reaction time in the industry, requesting automatic takedowns 24/7.

This is possible because the Axur platform acts on four layers: in addition to detection, the inspection, automation and removal technologies greatly reduce the mean time to containment (MTTC) for security teams. In addition, our Cyber Intelligence experts expand their research into both the Surface and the Deep & Dark Web.

Get started for free!

Book a demo now



///AXUR

Digital
experiences
made safe

axur.com