///AXUR

Threat Landscape

→ 2024/2025

A message from Axur

Threats evolve every year, but 2024 stands out for its defining characteristics: the deep integration of Artificial Intelligence (AI) in cybersecurity and the ever-expanding scope of risks it brings.

Malicious actors have exploited generative AI to craft highly convincing phishing campaigns and automate attack vectors at an unprecedented scale. However, AI was also a powerful ally in defense, capable of confronting threats with unparalleled coverage, speed, and prioritization.

As you'll see in the chapters ahead, AI even plays a role in shaping insights for reports like this, offering a glimpse into how technology can collaborate in building resilience against the challenges we face.

In parallel, ransomware remains a persistent menace. This year we've seen the rise of new access vectors, including increasingly complex supply chain attacks, while cyberblackouts tested the resilience of our systems. And still, amidst the chaos, we witnessed collaboration.

2024 demanded more from all of us. It forced us to rethink not just the tools we use, but the very philosophy of how we defend against what lies ahead. For me, it was a year that reinforced my belief in our mission: to create safer digital experiences, harnessing the transformative power of technology to connect, respond, and adapt faster than ever before.

We invite you to explore this report, where we analyze these evolving threats, outline strategic responses, and share insights to empower your team to thrive in this complex landscape. Not just to understand the challenges, but to embrace the opportunities they create.

To build resilience, and to ensure that as technology transforms, it does so in service of a safer, stronger digital future.

Let's step forward together.

Fábio F. Ramos
CEO at Axur

Table of Contents

Executive Summary 04

Threat and Exposure Landscape 08

2024 in Numbers 18

Trends for 2025 35

Recommendations 40

Fraud Neuron 45

About Axur 49

Executive Summary

13x more credentials detected, totaling **57.2 billion**

339 million credit and debit cards detected, **26x more** than in 2023

Phishing cases doubled, with **72,455** malicious pages detected. Insights reveal that **70% of fraudulent pages** lacked domain-related keywords

439,000 fraud incidents reported, a 118% increase compared to the previous year, including fake profiles, fraudulent apps, and brand impersonation

2.3 billion messages analyzed in the Deep & Dark Web, leading to **over 966,000 incidents**

32% of all Deep & Dark Web incidents involved audiovisual content, such as audio, video, and static images

More than 401,000 fraudulent pieces of content removed through automated takedown workflows

Fake profiles and information exposure widely used to target executives and VIPs, with over **33,000 incidents reported**

→ Healthcare ransomware:
Attacks disrupted critical services in the U.S. and U.K.

→ The largest in history:
Cloudflare blocks a record-breaking 3.8 Tbps DDoS attack.

→ Operation Cronos:
Global initiative weakened the LockBit group, marking progress in combating ransomware.

→ AT&T and Snowflake:
Breach exposed millions of records, revealing vulnerabilities in telecommunications.

→ Falcon failure:
Issues with CrowdStrike's sensor caused disruptions and exposed interconnected vulnerabilities.

Most Targeted Sectors

→ Retail/E-commerce

#1 in phishing: 27,305 fraudulent pages detected
#3 in Deep & Dark Web incidents: 172,873 incidents
#3 in takedowns: 61,343 fraudulent contents removed

→ Finance/Insurance

#1 in takedowns: 107,601 fraudulent contents removed
#2 in phishing: 15,051 fraudulent pages detected
#2 in Deep & Dark Web incidents: 257,275 incidents

→ Technology

#1 in Deep & Dark Web incidents: 418,806 incidents
#3 in phishing: 9,502 fraudulent pages detected

→ Telecommunications

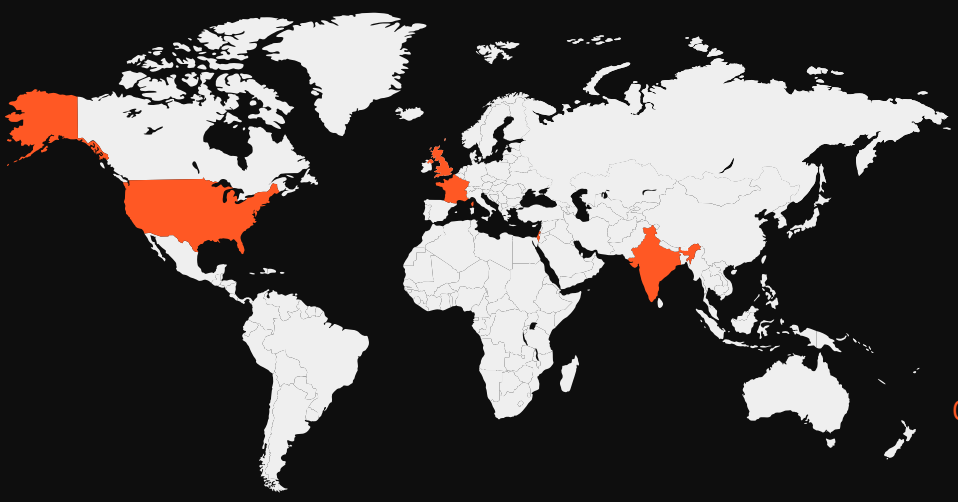
#2 in takedowns: 93,287 fraudulent contents removed
#4 in Deep & Dark Web incidents: 47,018 incidents

→ Travel & Tourism

#5 in takedowns: 45,060 fraudulent contents neutralized

Most Impacted Locations

Top 5: The U.S., India, the U.K., France, and Israel were the most targeted by cybercriminals in 2024.



Emerging Trends

→ AI in cybercrime:
Deepfakes and personalized attacks driven by GenAI.

→ Expansion of attack surfaces:
IoT devices and BYOD policies increase vulnerabilities.

→ Sophisticated infostealers:
Credential and cookie theft become more versatile.

→ Cybersecurity as a national priority:
Geopolitical tensions reinforce the need for robust security approaches.

Recommendations

→ Identity management:
Monitor and revoke compromised credentials, complementing MFA with continuous analysis.

→ EASM and vulnerabilities:
Prioritize critical vulnerabilities using threat intelligence insights.

→ Continuity planning:
Map critical dependencies to ensure operational resilience.

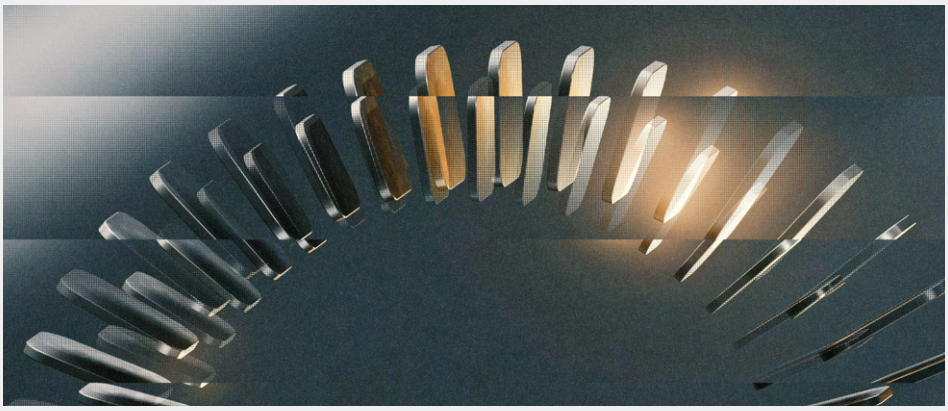
→ Awareness programs:
Strengthen security culture with organizational education initiatives.

New Fraud Framework Available

Fraud Neuron enables seamless information sharing and structured modeling of digital fraud, bridging security and anti-fraud teams.

Read now

Threat and Exposure Landscape



The cybersecurity landscape in 2024 has emerged as a dynamic and challenging battlefield.

Ransomware attacks remain a critical concern, with groups refining their tactics and targeting essential sectors such as healthcare and infrastructure. Additionally, the rise of identity-based attacks, driven by sophisticated phishing and social engineering techniques, highlights the need for robust defenses.

Cloud vulnerabilities are also on the rise, reflecting an increasing reliance on these services.

An analysis of the most exploited CVEs revealed a significant uptick in the exploitation of critical vulnerabilities, with cybercriminals taking advantage of weaknesses in widely used systems. Malware has demonstrated a capacity to compromise sensitive data, while the most utilized tactics include DDoS and phishing attacks, which are being executed with greater sophistication and frequency.

Axur's AI-powered threat intelligence (CTI) solution processes and summarizes thousands of alerts and hours of research into actionable insights, delivering only the most relevant information tailored to specific attack surfaces or predefined topics of interest.

This advanced technology shaped the insights in this chapter, featuring comments from Alisson Moretto, Head of Cyber Threat Intelligence at Axur.

44 thousand

articles analyzed

6 thousand hours

of threat research

Reviewed and commented by:

Alisson Moretto

Head of Cyber Threat Intelligence at Axur

> Extensive experience in digital crime investigation and incident response

> Guest lecturer for graduate programs and speaker at prominent industry events

Top Insights for 2024

Click on the titles to view full analysis

↗ Cyberattack on Change HealthCare disrupts U.S. prescription services

This incident underscores the vulnerability of healthcare systems to cyberattacks, affecting critical services across the U.S. and raising concerns about patient safety and data integrity.

↗ Qilin ransomware disrupts NHS blood services in London

The attack on vital healthcare services demonstrates ransomware's potential to paralyze vital public operations, affecting patient care and emergency services.

↗ Cloudflare stops biggest DDoS attack in history

Cloudflare mitigated a record 3.8 Tbps DDoS attack using compromised IoT devices and targeting multiple industries, highlighting the growing sophistication of global cyberthreats.

↗ AT&T data breach exposes call records via Snowflake infiltration

This massive data leak raises serious privacy concerns for millions of customers and highlights vulnerabilities in telecommunications infrastructure.

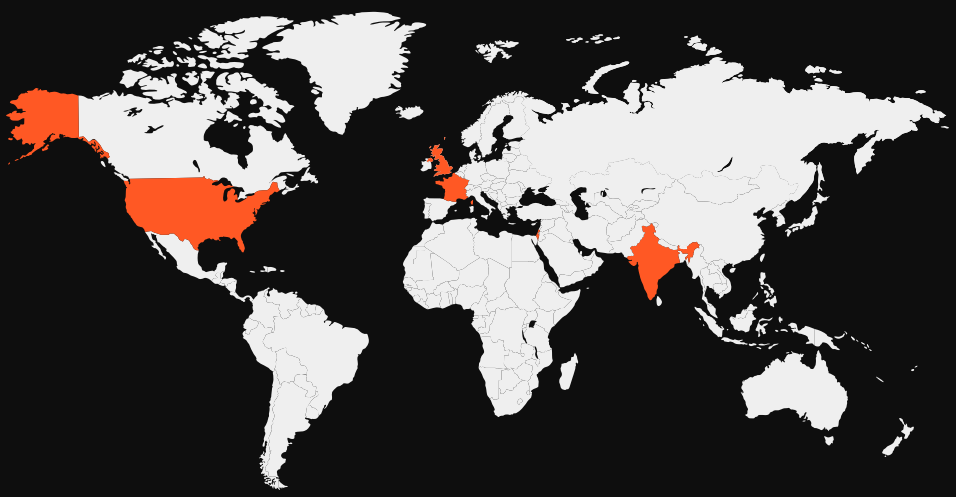
↗ Operation Cronos dismantles LockBit's ransomware network

This operation represents a significant law enforcement effort aimed at combating ransomware by targeting one of the most notorious groups in the cybercrime landscape, which could deter future attacks.

↗ Global failure of Falcon exposes interconnected vulnerabilities

A flawed update of CrowdStrike's Falcon sensor led to BSOD errors in critical systems, prompting phishing attacks and underscoring the need for rigorous quality controls and cyber resilience.

Most Impacted Locations in 2024



The United States, India, the United Kingdom, France, and Israel were among the most targeted locations by threat actors in 2024, driven by a combination of geopolitical factors, technological vulnerabilities, and the overall surge in malicious cyber activities.

Geopolitical tension, especially in the Middle East, played a significant role. Israel, for instance, became a frequent target of attacks, partly due to its strategic alliance with the U.S. and ongoing tensions with nations like Iran.

In 2024, Israel received military and cyber support from the U.S., the U.K., and France to fend off Iranian cyberattacks, intensifying attention from hostile groups like RipperSec.

Government, education, and healthcare sectors in countries like the U.S. and the U.K. were particularly vulnerable to attacks due to their handling of sensitive data and exploitable infrastructures. Moreover, the transition to hybrid and remote work has increased security gaps, allowing attackers to exploit flaws in email systems and corporate networks.

The motivations behind these attacks range from espionage to financial extortion. Ransomware continued to be a common tool for demanding ransoms in cash or cryptocurrencies. In April 2024, the U.S. led the records of such attacks. India was also identified as a significant target due to its growing digitization and strategic importance in the Asia-Pacific region.

Most Active Threat Actors

Throughout the year, the cybersecurity threat landscape saw the evolution and emergence of various groups, with some significant changes in their operations and impact:

The cyber environment in 2024 is marked by the continuous evolution of threat actors. Groups like RansomHub and ShinyHunters stand out for their aggressive operations and significant impact. Meanwhile, other groups like LockBit are struggling due to increasing pressure from authorities. Collaboration among hacktivist groups is also intensifying, signaling a new strategy in the cybersecurity threat landscape.

Active since: 2020

Motivation: Financial

Most affected sectors: Organizations in the United States and Europe, focusing on infrastructure and other industries

Country of origin: Russia

RansomHub ↗

This ransomware group is considered a reincarnation of the Knight ransomware. It quickly rose to one of the most prominent groups, especially after law enforcement actions against LockBit3, which significantly declined its activity. It was also responsible for a notable increase in victims in 2024. The group made over 210 new victims, according to the FBI, including companies like automaker Kawasaki and U.S. communications provider Frontier Communications, as well as leaking data from Change HealthCare after the BlackCat/ALPHV attack.

Active since: 2020

Motivation: Financial

Most affected sectors: Financial and other data-rich companies

Country of origin: Operates internationally

ShinyHunters ↗

This group gained attention after a massive attack on Ticketmaster, claiming to have stolen personal data from 560 million customers. The attack may have been one of the largest in history in terms of the number of victims and highlighted the group's capability to execute large-scale attacks.

Active since: 2023

Motivation: Political

Most affected sectors: Governmental organizations or companies in countries opposing its ideology

Country of origin: Malaysia

RipperSec ↗

This group stood out for its self-proclaimed DDoS activities targeting Israel and companies like X, Uber, Ferrari, and Paramount. Their campaign in support of Telegram founder Pavel Durov expanded rapidly under the name #FreeDurov, mobilizing various other hacktivist groups, reflecting a shift in collaboration dynamics among groups previously operating in isolation.

Active since: 2022

Motivation: Financial

Most affected sectors: Various, including government, telecommunications, energy, and others

Country of origin: Russia

Intelbroker ↗

While little new information emerged about Intelbroker's operations in 2024, this threat actor remains active in the scene, primarily in forums, sharing access credentials and sensitive data.

Active since: 2019

Motivation: Financial

Most affected sectors: Various, including industry, healthcare, education, and others

Country of origin: Russia

LockBit ↗

Following a series of successful law enforcement operations against LockBit3, the group experienced a significant decline in activity. The group was responsible for over 2,000 victims worldwide and extorted over $120 million in ransom payments. In 2024, a collaboration among 10 countries led to dismantling its infrastructure.

Highlighted CVEs in 2024

Ransomware groups have started exploiting this vulnerability to inject malicious payloads and install ransomware on vulnerable servers.

The patch should be applied by updating to versions 8.1.29, 8.2.20, or 8.3.8. Additionally, it is recommended to use the Argument Injection Susceptibility Checker, implement a Web Application Firewall (WAF), restrict access to PHP-CGI scripts, validate inputs, and conduct regular security audits.

A critical remote code execution vulnerability was identified in Veeam Backup and Replication software, affecting versions 12.1.1.2.172 and earlier, with a CVSS score of 9.8. Two patches were released to address the issue, with the second being a complete solution. The vulnerability is linked to deserialization attacks in an outdated communication engine and is heavily exploited by ransomware groups.

Discovered in SolarWinds Web Help Desk (WHD), this vulnerability allows unauthenticated attackers to access and modify ticket details, exposing sensitive data such as credentials and password reset requests. A hotfix has been released to address the issue.

This vulnerability in libcurl occurs when an application enables HTTP/2 server push, and the received headers exceed the 1000 limit. In such cases, libcurl aborts the push but fails to release all allocated memory, causing a silent memory leak that is difficult to detect. This vulnerability can lead to a denial-of-service condition.

Identifies an issue in the verification methods for IPv4-mapped IPv6 addresses. Methods such as IsPrivate and IsLoopback return incorrect results for addresses that would otherwise be valid in their traditional IPv4 forms.

This is an untrusted data deserialization vulnerability that can enable remote code execution (RCE) with a malicious payload, even without authentication.

Discover deeper CVE insights with Axur

Start your free trial of our AI-powered Cyber Threat Intelligence solution and uncover the most relevant threats of 2024.

Get a Demo

Most Active Malware in 2024

In 2024, the malware landscape is marked by increased attack sophistication and the prevalence of ransomware-as-a-service (RaaS). Well-known groups continue to evolve their strategies to maximize financial impact on victims.

Most Utilized TTPs

T1078 - Valid Accounts

This technique refers to the use of legitimate credentials to gain access to systems. Attackers frequently exploit valid accounts to avoid detection and maintain access to compromised networks, especially in environments where credentials are often reused or poorly managed.

T1190 - Exploitation of Public-Facing Applications

Covers the exploitation of applications that are publicly exposed on the internet. Attackers can exploit vulnerabilities in web systems to gain initial access to corporate networks, a critical issue for organizations that delay patching vulnerabilities.

T1071 - Application Layer Protocols

Involves using application layer protocols to communicate with command-and-control (C2) servers. Attackers use this technique to exfiltrate data or receive instructions without raising suspicion, leveraging common protocols like HTTP or HTTPS.

T1059 - Command and Scripting Interpreter

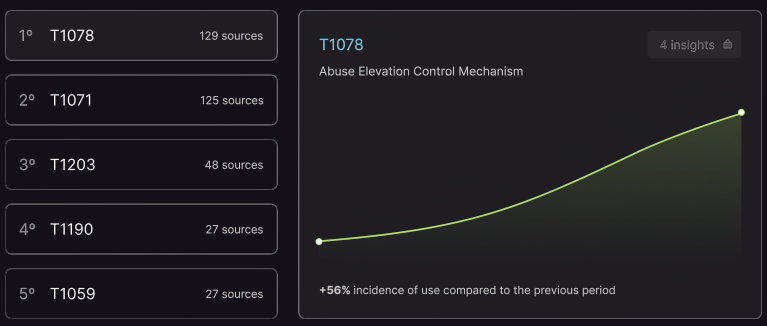
Involves the use of command and scripting interpreters to execute malicious code. This includes using languages like PowerShell, Bash, or Python to perform malicious actions on the target system. This technique is common in attacks that aim for automation or remote execution to bypass security controls.

T1203 - Exploitation for Client Execution

Refers to exploiting vulnerabilities in client software to execute malicious code. This can occur by opening malicious documents or email links, leading to unauthorized execution. This technique is often used in targeted attacks where users are induced to perform actions that compromise their systems.

T1566 - Phishing

Encompasses phishing attacks where attackers attempt to deceive users into revealing sensitive information, such as credentials or financial data. This technique remains one of the most prevalent due to its high success rate and low cost for attackers.

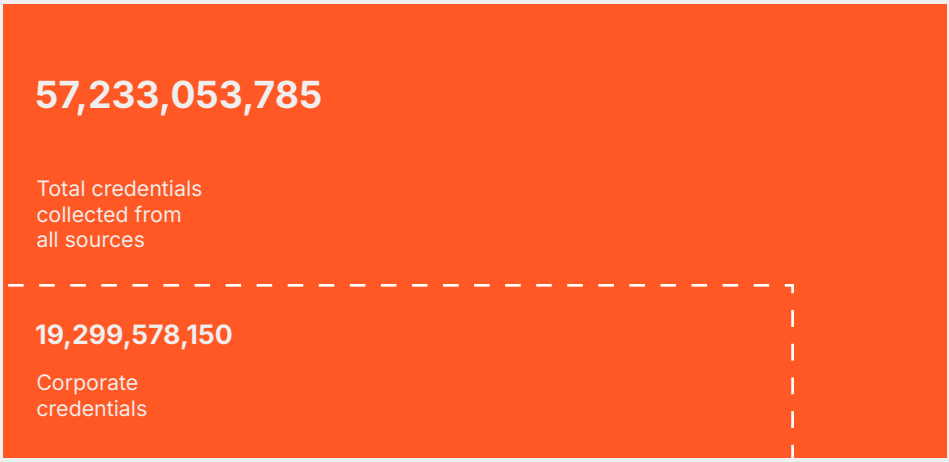


2024 in Numbers

Credentials

The Axur platform detected 57.2 billion leaked credentials throughout 2024, highlighting the critical need for assertive and efficient identity management to protect online services and corporate networks.

Axur's detections are based on activity in the Deep & Dark Web and files shared on the open web, including forums frequented by hackers. For this reason, it can be asserted that all these credentials are already in the hands of cybercriminals. If these credentials are not revoked and replaced, the accounts will remain at risk.



Additionally, almost all credentials (98%) are shared without any encryption. This indicates that cybercriminals are using techniques to find passwords that match leaked hashes (like MD5 and SHA) or are obtaining unencrypted passwords through infostealers.

According to the 2024 Verizon Data Breach Investigations Report (DBIR), 31% of all access breaches in the last ten years were due to stolen credentials.

However, over 70% of unauthorized access cases occurred because of weak or previously compromised credentials in certain attack categories—such as account takeovers on web platforms.

The Threat of Infostealers

3.2 billion credentials were obtained by infostealers in 2024

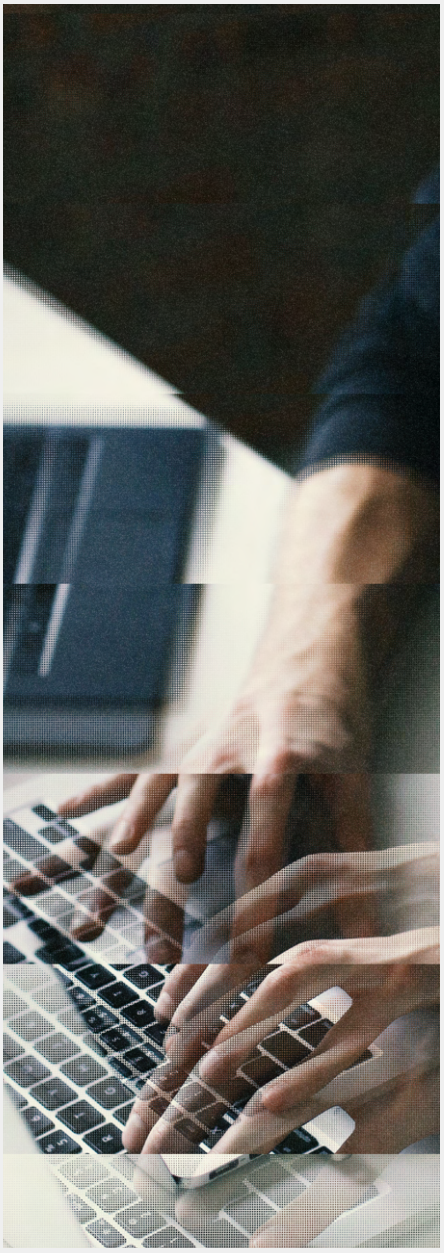
Infostealers are a malware category encompassing programs created to steal credentials. Several families of infostealers are continuously refined to evade antivirus detection.

Unlike traditional keyloggers, which operate passively and wait for users to access a system to steal passwords, infostealers are programmed to actively search for and extract all system information.

Whenever possible, infostealers access passwords stored in web browsers, password managers, and applications installed on the computer (digital wallet managers, software distribution platforms, gaming platforms, and others). Infostealers can also steal cookies stored by browsers.

The theft of cookies and access tokens by infostealers enables session hijacking attacks. By leveraging an already authenticated session, attackers can bypass multi-factor authentication (MFA) requirements.

Infostealers can be disseminated through social engineering campaigns, pirated software, and phishing. Stolen passwords are often sold to other specialized criminals—while financial scams can exploit banking credentials or digital wallet keys, ransomware attacks may leverage VPN or remote access service credentials.



New Rules for Credentials

In addition to being stolen by infostealers, unencrypted passwords can also be obtained through brute force attacks and credential stuffing, where reused passwords across multiple services are validated to find other accounts using the same combination.

Encrypted or hashed passwords can also be compromised using previously computed values in Rainbow Tables or cracked over time as computational power increases.

In this context, the definition of a "strong password" is no longer the same. In September, the National Institute of Standards and Technology (NIST), a U.S. government regulatory body, issued a revision of its Password Guidelines document with updated recommendations tailored to this reality for federal government entities.

Overall, the guidelines now favor a more proactive approach by organizations in blocking compromised credentials rather than rigid rules such as periodic password changes.

Passwords should also be longer to prevent brute force attacks and safeguard against protective mechanism failures.

☑ What Is Now Recommended

→ **Revoke compromised passwords:** authentication systems should revoke compromised passwords and prevent users from using notoriously unsafe passwords. New account registrations with compromised passwords should also be blocked.

→ **Use passwords of at least 15 characters:** Users should be encouraged to use longer passwords. No system should accept passwords shorter than 8 characters.

→ **Allow up to 64 characters:** Systems should not impose strict limits on creating short passwords. They should permit at least 64 characters to accommodate users who prefer passphrases.

☒ What Is Not Recommended

→ **Periodic password changes:** instead of enforcing periodic changes, organizations should focus on revoking compromised passwords and adopting MFA. Mandatory periodic changes often lead users to choose weaker passwords, compromising their resilience against brute force attacks.

→ **Use of special characters or "complex" passwords:** with the transition to longer passwords or passphrases, password entropy is naturally higher than when using special characters. However, NIST recommends that systems accept any Unicode character.

→ **Password hints:** "secret questions" and "hints" for forgotten passwords should not be used, as attackers can exploit these same features to uncover passwords.

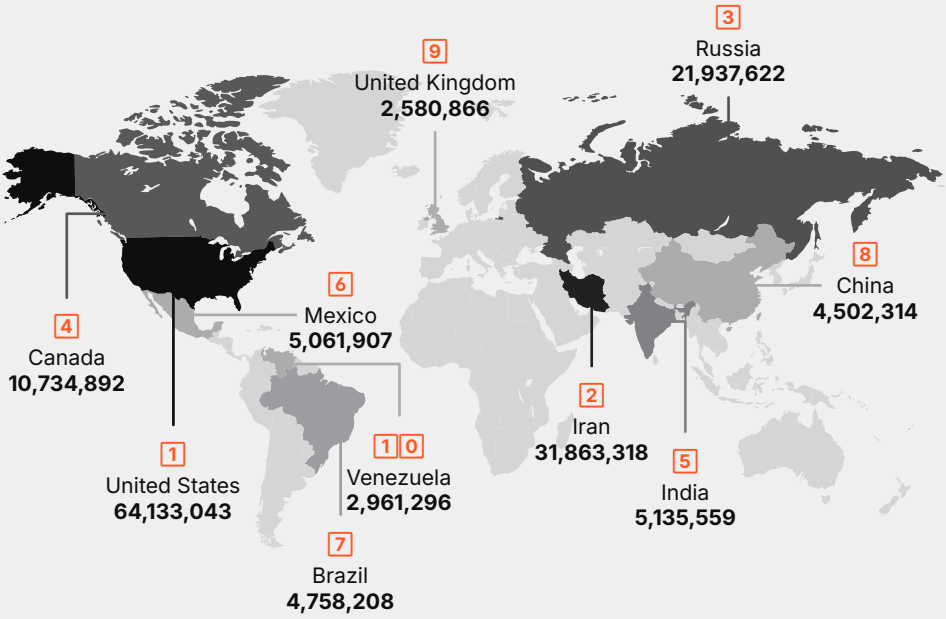
Payment Cards

Cybercriminals shared 339 million credit and debit cards in 2024

Growth in Exposed Cards

2023	**13.5 million**
2024	**339 million**

The volume of stolen cards remains high. Using the Bank Identification Number (BIN), it is possible to estimate the origin of each leaked card. The U.S. cards, with high purchasing power, still rank first on this list.



The theft of payment cards impacts financial institutions and e-commerce businesses, which often absorb the losses for goods and services purchased with stolen cards.

Axur monitors these leaks to help companies block the use of compromised cards.

Phishing

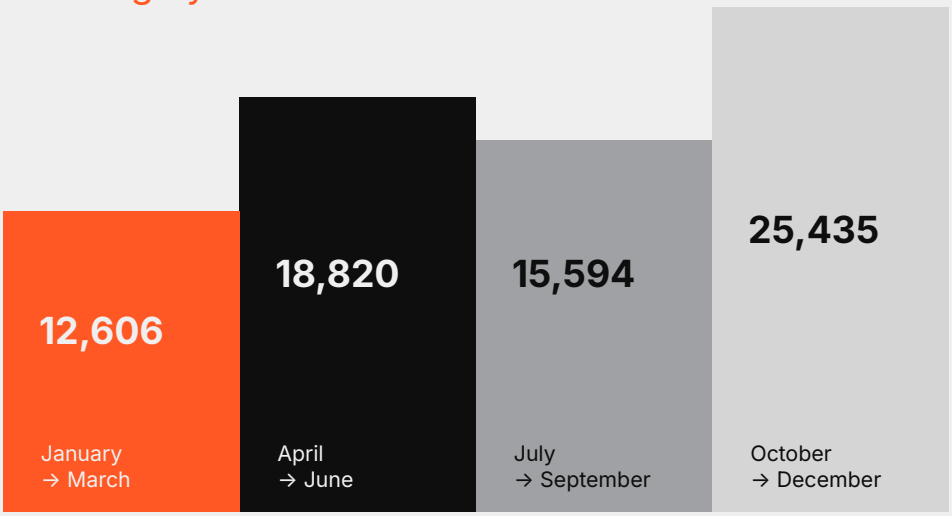
The volume of detected phishing pages doubled in 2024, reaching 72,455

Detecting phishing pages is a crucial step in combating online fraud. Axur's monitoring focuses on identifying pages where victims may be tricked into providing sensitive information.

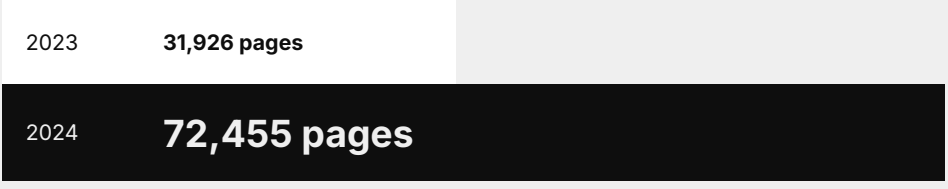
This focus is particularly relevant in the mobile environment, where scams frequently exploit well-known brands through app ads or SMS campaigns.

Identifying and eliminating these pages is essential to mitigating risks and protecting consumers in spaces where much of today's financial and retail activity occurs.

Phishing by Quarter



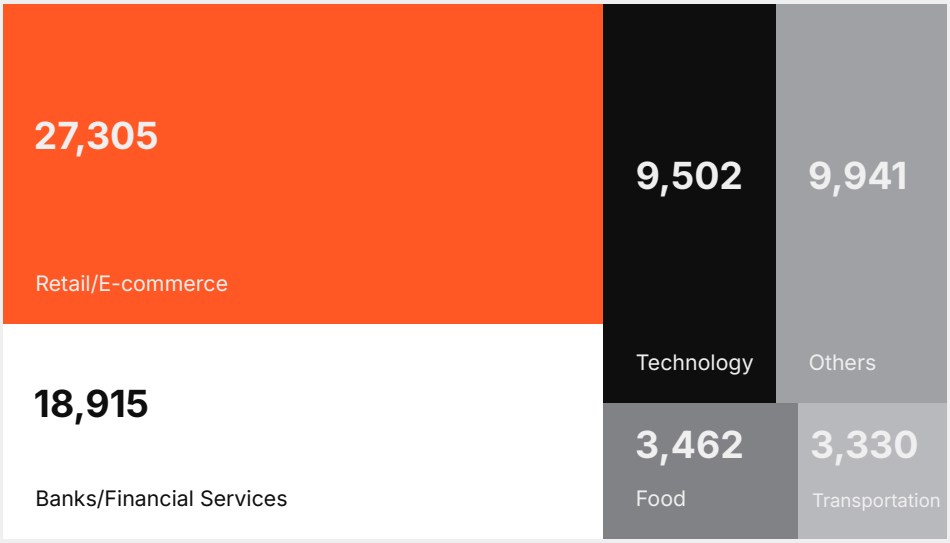
The growth of phishing pages



The retail and e-commerce sector remains the most targeted by phishing attacks, followed by financial institutions. Cybercriminals often use stolen accounts to make fraudulent purchases or steal personal information.

Additionally, retail brands are frequently leveraged as vehicles for stealing credit card details, which can then be used to buy goods or services.

Phishing by Sector



70% of phishing scams avoid using keywords in the domains

18% exclude keywords from the page's HTML code

How LLMs are Redefining Threat Detection

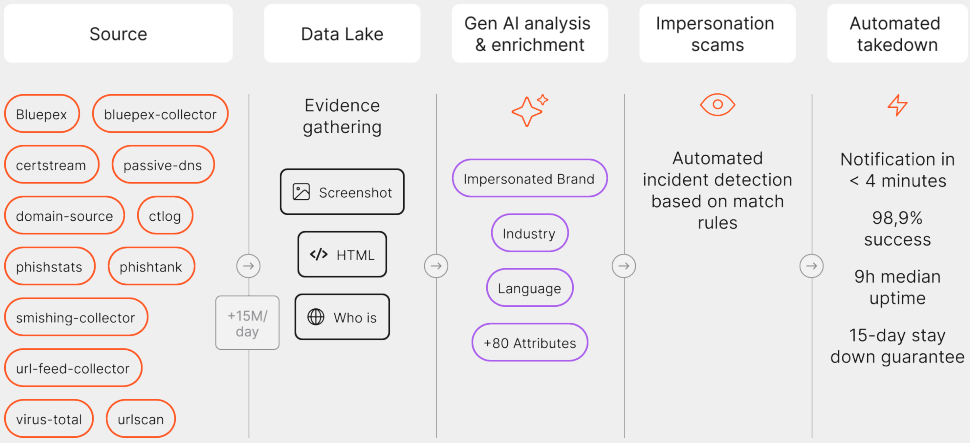
Axur has taken a leap forward in identifying digital threats with Clair LLM (Cyber Lens for Anomaly and Impersonation Recognition), a proprietary model based on generative AI. Unlike traditional solutions, Clair leverages Vision Language Models (VLMs) developed in-house and trained with over 15 years of data and expertise in detecting fraudulent content. This innovative approach combines textual and visual analysis to inspect more than 15 million websites daily, significantly enhancing the ability to detect sophisticated fraud.

The model processes URLs, evaluates page content, and generates detailed descriptions. It identifies present brands, detects requests for credentials, payments, or passwords, and assesses whether an attempt to impersonate a specific brand occurs.

All of this is done automatically, without human intervention. This accuracy results directly from integrating enriched data and detailed analyses, surpassing simple keyword-based detection. Using proprietary models also ensures that all data processed remains within Axur's infrastructure, maintaining privacy over analyzed information.

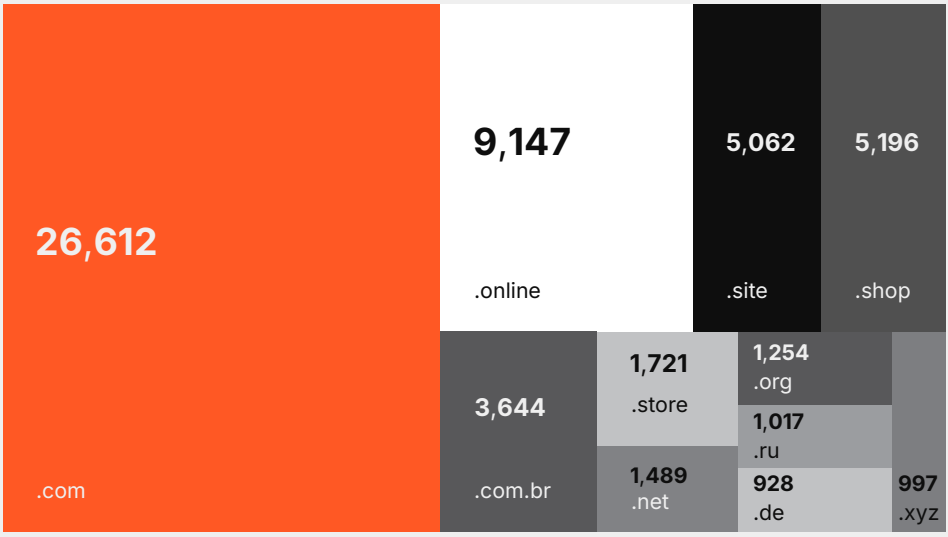
With the Threat Hunting tool, cybersecurity and anti-fraud teams leverage Clair's mechanism to deeply investigate phishing campaigns, applying customized filters that increase visibility into attacks—all without compromising the efficiency of automated detections.

A fundamentally new approach to brand protection



Use of Top-Level Domains (TLDs)

In 2024, there was a rise in fraud linked to TLDs such as ".shop" and ".store", reflecting the prevalence of phishing scams targeting retail and e-commerce.



TLDs are the suffixes of web addresses, such as ".com" (available to anyone), ".gov" (reserved to U.S. government websites), or ".uk" (country-specific suffixes). In the past, TLDs were tightly controlled, with only a few institutions authorized to operate them—typically representing regions or countries (e.g., ".br," ".de," ".jp," ".ar").

Since 2012, procedures have allowed for the request of generic top-level domains (gTLDs), enabling the creation of new suffixes. Each TLD is managed by a registry, which may choose to sell subdomains to offset infrastructure and registration costs.

As the process of requesting a gTLD is expensive and highly bureaucratic, cybercriminals must select from existing TLDs to register a domain that enhances the reach or credibility of their fraud.

This selection is especially critical for phishing websites, as victims often scrutinize webpage addresses.

Factors influencing this choice include:

→ Victim's familiarity with the domain

Most internet users are accustomed to visiting sites ending in ".com." However, the most popular suffixes are those with limited new registrations availability.

→ Domain availability

Short addresses, simple words, or trademark names are no longer available under traditional TLDs. Cybercriminals may attempt to find these names under newer gTLDs or similar alternatives.

→ Connection to the scam

Many gTLD suffixes are thematic, such as ".shop." A criminal may decide that a specific suffix makes the fraud appear more convincing.

→ Cost

Some TLDs are more expensive than others. For restricted TLDs like ".edu" or ".gov," which cannot be registered, cybercriminals may resort to hacking legitimate websites with these suffixes to host their scams.

→ Registrar policies and fraud response

All domain registrars must adhere to specific rules. However, differences in handling particular cases may influence cybercriminals' preferences, as these affect how long their fraud remains active online.

DPN Analysis		
DPN	2023	2024
.com	32.9%	36.65% ↑
.online	19.6%	12.6% ↓
.shop	16.9%	7.16% ↓
.site	7.3%	6.97% ↓
.com.br	5.6%	5.02% ↓
.store	5.1%	2.37% ↓

Takedowns Executed

401,000 cases of fraudulent content were removed thanks to Axur's notifications

As phishing becomes more sophisticated and expands to new channels, such as SMS and in-app advertising, the response to remove malicious content becomes critical.

Identifying a phishing page is only the first step in mitigating risks—a well-structured, swift takedown notification is essential to minimize the exposure time of a scam.

In 2024, over 401,000 takedowns through Axur's notifications, each directed at the infrastructure providers, social media platforms, or hosting services used by criminals. This scale was achieved through a highly automated process supported by artificial intelligence, which not only accelerates notification dispatch but also compiles the necessary evidence to ensure a higher success rate.

The effectiveness of these requests relies on a precise and technical approach: identifying the correct provider, presenting clear evidence, and adhering to the required formats. While automated processes significantly streamline this, success is also tied to the credibility Axur has built over years of consistent and reliable notifications, reducing delays in execution.

Additionally, during the interval between notification and removal, proactive measures such as alerts to browsers and security providers help limit the impact of the fraud, protecting potential victims.

This combination of strategies is critical to maintaining a high success rate for takedown requests.

Takedowns

401k	98,9%	4 minutes	9 hours
requested takedowns	Success rate	median time to 1st notification	median resolution time

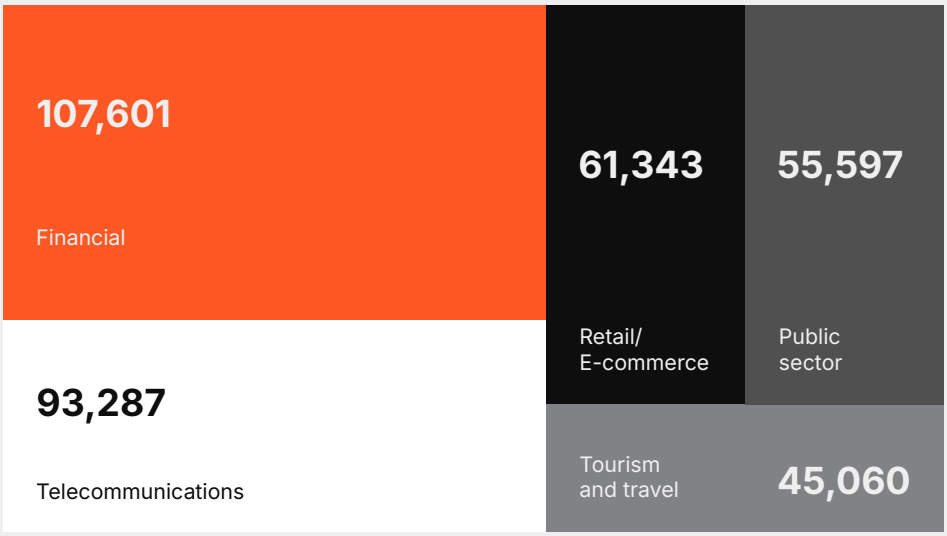
Detect, analyze, and remove threats faster than ever

- Completely automated takedown 24/7
- Notification in <4min
- 98.9% success
- 9h median uptime
- 15-day stay down guarantee
- Web Safe Reporting
- Complete transparency so you can follow up the whole process
- We charge only for successful takedowns

Most Affected Sectors

In 2024, the financial sector led with 29.8% of all cases, resulting in over 107,000 notifications. Telecommunications and retail/e-commerce combined accounted for 42% of incidents, totaling approximately 154,000 pages removed.

Other industries, such as tourism and the public sector, also faced significant challenges, with over 100,000 fraudulent pages neutralized.



Deep & Dark Web

Axur analyzed 2.3 billion messages across Deep & Dark Web channels to provide intelligence on cyber threats and incidents

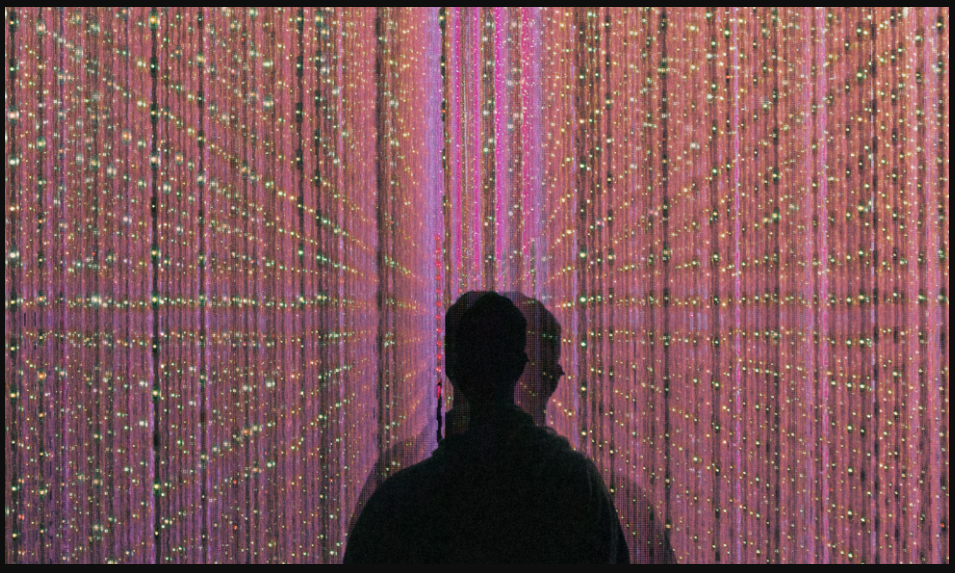
Cybercrime today is a complex ecosystem connecting individuals and groups involved in cyberattacks. These communication channels exist to make crime more efficient and maximize illicit profits.

However, these spaces present an opportunity to collect intelligence and track the activities of malicious actors.

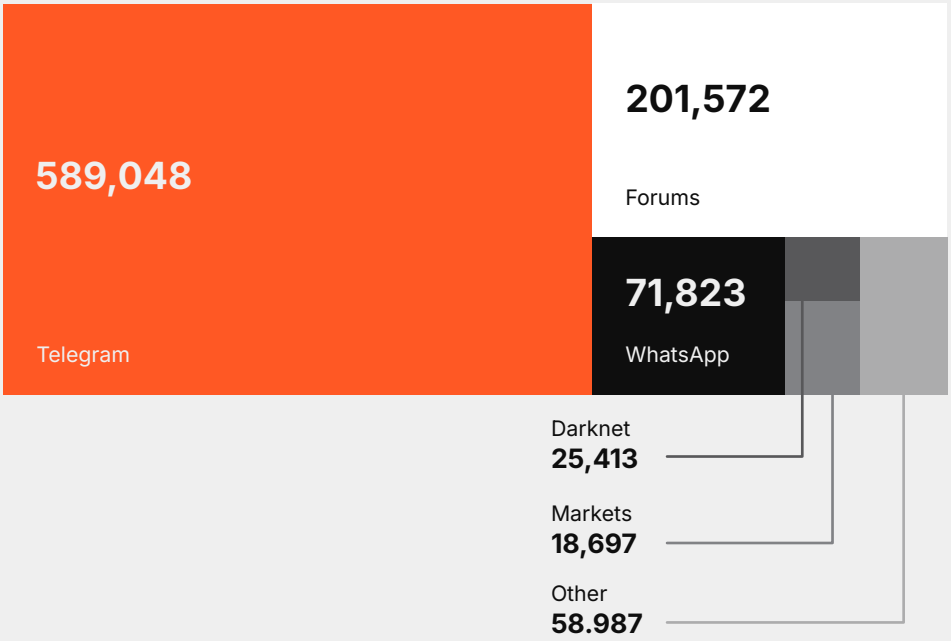
Axur has access to numerous such environments, monitoring criminal communications to identify discussions indicating potential data exposure incidents, vulnerabilities, or fraud campaigns.

From this analysis, Axur identified 966,170 incidents, demonstrating that the key to extracting actionable intelligence lies in filtering and interpreting the collected material into meaningful alerts.

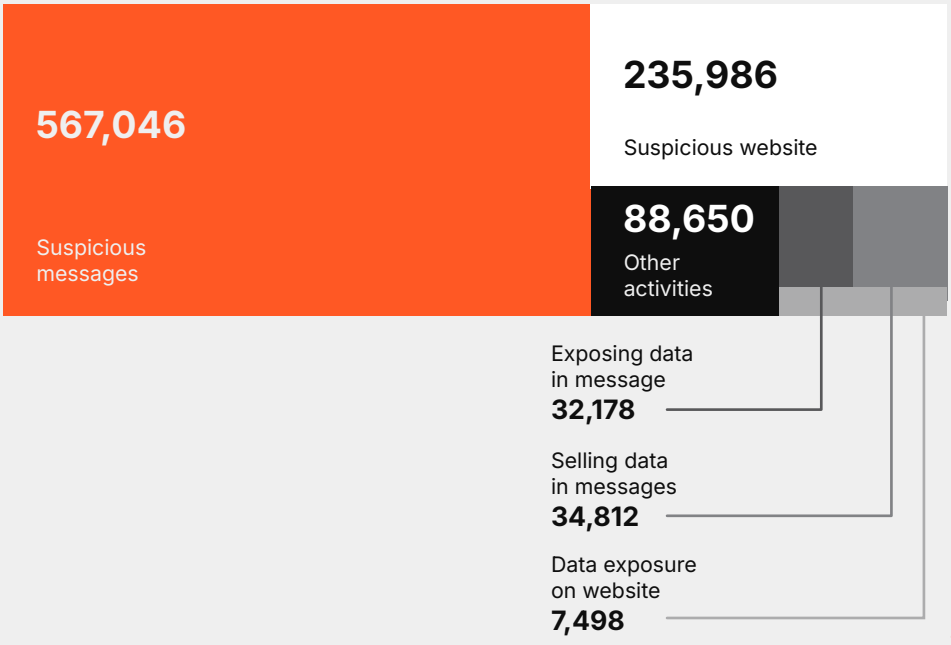
We converted the analysis of messages into 966,170 incidents — the key to extracting intelligence lies in filtering and interpreting the material collected from alerts.



Deep & Dark Web Sources



Detection Types



Deep & Dark Web Incidents by Sector

Sector	2023	2024
Retail	45%	18% ↓
Financial	26.1%	25% ↓
Technology	16.8%	44% ↑
Telecommunications	4.8%	5% ↑
Tourism	3.6%	2% ↓
Others	3.7%	6% ↑

Audiovisual Content

In 2023, approximately 25% of Deep & Dark Web incidents were detected in audiovisual content. The analysis of this material, aided by artificial intelligence for transcribing audio and converting images into text, became even more significant in 2024, as nearly half of the communications analyzed were in audiovisual formats.

68%

Text-based content

32%

Audio, video, and images

Fake Profiles, Illegitimate Apps, and Fraudulent Brand Use

We detected nearly half a million digital fraud attempts using sophisticated strategies to deceive consumers

In 2024, Axur identified over 439,000 digital fraud cases, including fake profiles, illegitimate apps, fraudulent brand use in paid searches, similar domain names, and other improper associations. These incidents represent diverse strategies used by criminals to deceive consumers and compromise companies' reputations.

151,119 fake profiles on social media platforms

262,575 cases of fraudulent brand use

20,934 illegitimate mobile applications

Fake social media profiles, totaling 151,000 cases, are often used to promote phishing pages or deceive followers of legitimate accounts into providing sensitive information or making fraudulent payments.

Of the fake profiles reported by Axur in 2024, **over 80%** were taken down in partnership with Meta Ads, responsible for Facebook and Instagram, totaling more than **57,000 takedowns through Axur's automated workflows.**

With Mark Zuckerberg's changes to the platforms' moderation policies, it will be essential to monitor the impact on future removals.

Learn more ↗

The 20,000 illegitimate apps detected leveraged the mobile environment, requiring additional user interactions after installation, such as granting permissions to access data or monitor device activities, thereby amplifying the reach and impact of fraudulent schemes.

Executives & VIPs

Executives are often prime targets for digital fraud due to their influential positions and access to sensitive information. Criminals use social engineering to exploit their networks, whether through fake social media profiles or scams to deceive employees and partners.

These attacks aim to collect confidential information, such as access credentials, corporate credit cards, and strategic data, which can be used in targeted attacks.

→ Misuse of images: image editing software has long allowed for overlaying faces onto other images. However, the ease of reaching large audiences through cheap online advertising makes the systematic exploitation of public personalities feasible.

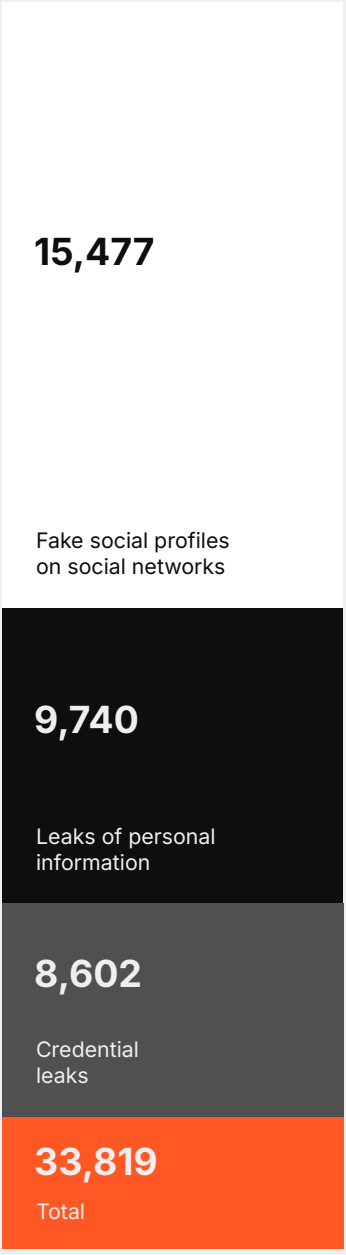
Deepfake technology, powered by artificial intelligence, has expanded the methods available for such activities.

Misusing the image and likeness of public figures can be used to target companies in phishing scams. Still, it can also be used solely to promote products or services improperly, generating an undue association of an individual with a fact or product and deceiving consumers.

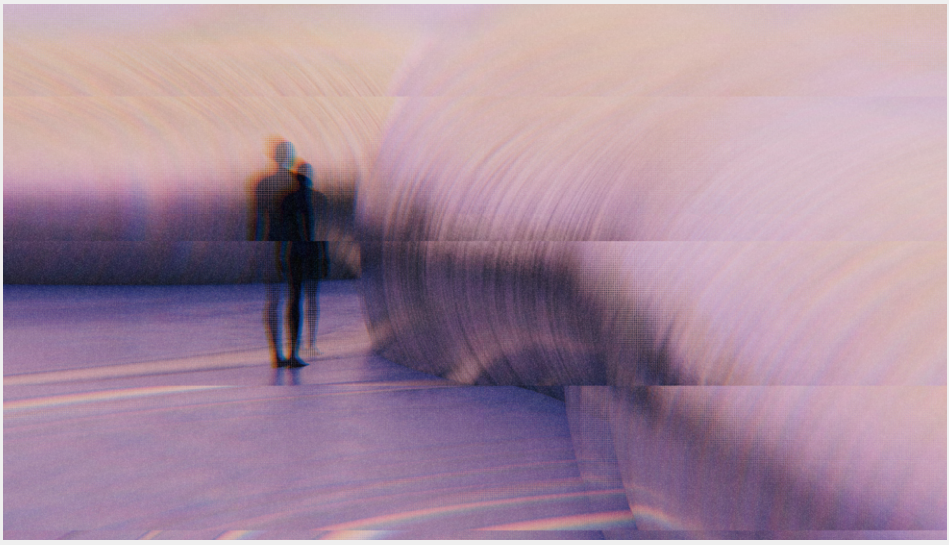
→ Exposure of confidential data: another critical risk is the exposure of confidential information, such as corporate credentials and credit card details, often found in leaks on the deep and dark web.

This data can be used to access internal systems, carry out financial transactions, or plan targeted attacks.

Axur detected over 33,000 incidents involving Executives and VIPs in 2024



Trends for 2025



↗ Artificial Intelligence (Still) at the Forefront of Trends

↗ Ransomware: New Players and Regulations

↗ New Authentication Methods and Attacker Adaptation

↗ Phishing: Expanding Tactics and Sophistication

↗ Cybersecurity vs. National Security

↗ Expanding Attack Surfaces

Artificial Intelligence (Still) at the Forefront of Trends

The potential of generative AI is solidifying its role in both defending corporate networks—through Cyber Threat Intelligence (CTI) solutions—and enabling digital fraud with deepfakes and personalized victim targeting. However, GenAI is not the only way to leverage Deep Learning algorithms.

AI continues to surprise and requires close monitoring. Early cybersecurity solutions are already employing AI to generate advanced analytics, and this same capability might be leveraged by criminals to create a market for curating leaked data.

We can expect GenAI algorithms to improve further—facilitating more sophisticated fraud involving fake identities. Additionally, vulnerabilities in AI platforms themselves could be exploited, as seen with a flaw discovered by Wiz analysts that allowed command execution and unauthorized access to other customers' data on an "AI-as-a-service" platform.

Moreover, ransomware is also expected to evolve significantly with AI, enabling faster, more precise, and targeted executions. With advanced algorithms, these threats will become harder to detect and contain.

Ransomware: New Players and Regulations

Law enforcement operations and internal conflicts considerably impacted ransomware groups LockBit and BlackCat in 2024. However, other criminal organizations have quickly filled the void left by these groups, highlighting the resilience of the "ransomware-as-a-service" (RaaS) model and the attackers' sustained interest in this lucrative fraud method.

Since mid-2024, authorities have been considering stricter regulations to make ransom payments more difficult—or even illegal. Insurers are also under pressure to stop covering such payments, as many believe ransom payments incentivize criminal behavior.

Organizations must stay ahead of these developments by focusing on incident prevention and recovery, ensuring their systems are resilient to ransomware attacks. Monitoring changes in cyber insurance policies and legislation will also be crucial.

New Authentication Methods and Attacker Adaptation

While many companies still struggle to implement multi-factor authentication (MFA), technology has already moved to the next step with passkeys. However, a definitive authentication method remains elusive.

In general, new authentication methods often mitigate ongoing attack strategies, forcing attackers to adapt. However, infostealers—malware that gained traction with the rise of MFA—are much more versatile than traditional phishing, capable of stealing cookies and bypassing MFA.

As a more adaptable attack, this means its evolution is likely to accelerate.

In 2025, hackers are likely to refine infostealers further. Additionally, attackers may increasingly target less familiar authentication channels, such as OAuth tokens and cloud applications, making them mainstream tools even among less skilled attackers.

Phishing: Expanding Tactics and Sophistication

Many attacks are being crafted around new phishing or social engineering techniques—whether leveraging deepfakes, physical threats, or ad fraud on social media platforms. The evolving narratives make it increasingly challenging to raise awareness and educate people about these scams.

From this perspective, phishing remains a key trend threat for 2025. Currently, 70% of malicious sites do not use the targeted brand name in their domains, and 18% do not even mention the brand in their HTML content. This requires advanced monitoring capable of detecting brand misuse solely in images or other subtle cues, increasing the need for specialized anti-fraud tools.

E-commerce platforms, financial institutions, and technology service providers will likely remain the primary targets of these attacks. However, phishing attacks against employees of organizations across all industries are becoming more common.

One way or another, this threat will continue to demand the attention and sophistication of fraud-combating and information security teams.

Cybersecurity vs. National Security

Geopolitical tensions are increasingly linking cybersecurity to national security. In 2024, many lawmakers began focusing on the entire technology supply chain, with the director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) stating that cybersecurity is a "software quality problem."

As many organizations create custom software or digital solutions, the technical rigor of the development process and information security measures may become market differentiators in the coming years. A robust cybersecurity posture could become both a commercial advantage and a contractual requirement.

Even if this does not materialize, the link between cybersecurity and geopolitics raises other concerns, such as hacktivist group activities.

Expanding Attack Surfaces

The proliferation of IoT (Internet of Things) devices and the adoption of BYOD (Bring Your Own Device) policies have significantly expanded organizations' attack surfaces. Every connected device, whether personal or corporate, can become a vulnerable entry point for cyberattacks. This challenge is exacerbated by the lack of consistent security standards in IoT devices and the increase in endpoints outside traditional corporate networks.

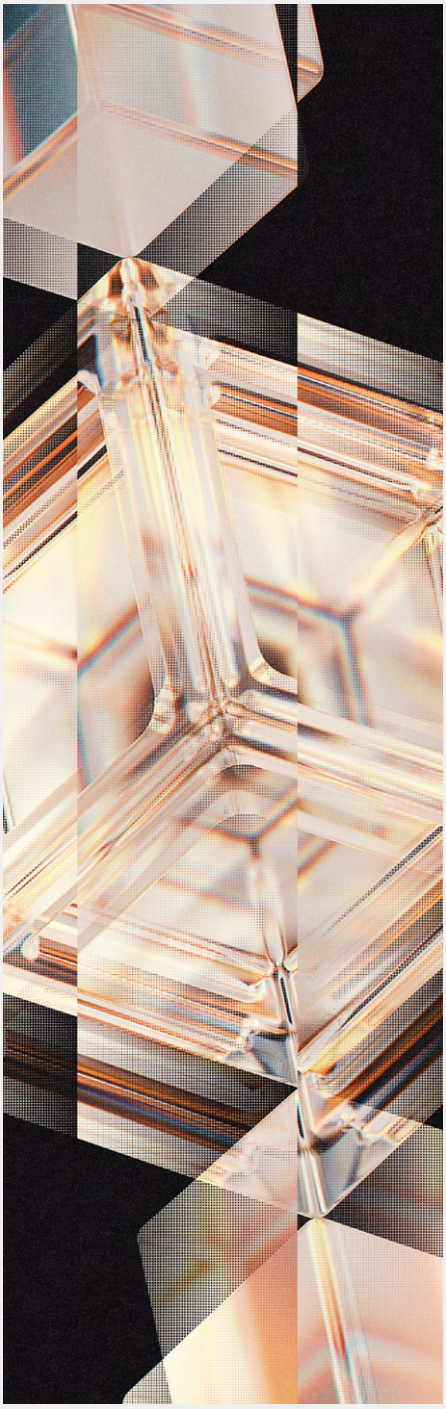
Mitigating these risks will require robust security measures, such as centralized device management, network segmentation to isolate less secure devices and frequent software updates. Additionally, clear policies for using personal devices and continuous monitoring solutions will be essential to quickly identify and respond to potential threats.

Recommendations

Identity Management

Inadequate identity and credential management proved to be one of the primary vulnerabilities for companies in 2024. Many organizations still strive to implement multi-factor authentication (MFA) across all access points. However, Identity and Access Management (IAM) policies must now consider cloud applications, API keys, and other access mechanisms often incompatible with solutions designed for human user credentials. Migrating these systems to a new authentication paradigm in the short term may not be trivial.

Monitoring leaked credentials is one of the most important tools for ensuring companies are one step ahead of attackers and can block credentials before they are exploited in attacks. This strategy is particularly beneficial for complementing MFA-based solutions or protecting systems undergoing migration.



Vulnerability Management

Exploitation of vulnerabilities remains one of the most common attack vectors for gaining access to corporate networks, indicating deficiencies in vulnerability management. The expansion of IT infrastructure and the decentralization of its management to specific business areas explain part of this issue. However, even the patch application itself can be ineffective when less critical vulnerabilities are addressed before more urgent ones.

Therefore, companies should adopt new methods to improve visibility into their IT infrastructure. A solution that combines External Attack Surface Management (EASM) with Artificial Intelligence alerts enables businesses to make informed decisions based on highly relevant insights into the most critical vulnerabilities, improving both visibility and patch prioritization.

Business Continuity Plan

When a company's operations depend directly on its IT infrastructure, the impact of cyber incidents tends to be more severe. There are already emblematic cases of businesses entering financial restructuring or shutting down operations following large-scale attacks. In 2024, for instance, MediSecure entered voluntary administration—a restructuring process for financially distressed companies in Australia—following a cyberattack, and National Public Data declared bankruptcy following the leak involving 2.9 billion records. The previous year, Rackspace was forced to discontinue its email service due to a ransomware attack.

This critical scenario aligns with the growing concern among companies: a recent Hiscox Cyber Readiness Report found that 35% of organizations consider cyberattacks one of the top five risks to their operations.

In this context, having a Business Continuity Plan is essential to ensuring organizational resilience under adverse conditions. The planning process itself can greatly benefit the company, as it requires mapping critical systems. Businesses should also assess their reliance on third parties and vendors, who may also be targets of attacks. Tools like Axur's Threat Hunting, which includes a database of over 42 billion credentials, are an effective way to map risks associated with third-party platforms and systems.

35% of organizations consider cyberattacks to be one of the top five risks to their business

Phishing Mitigation with Monitoring and Takedown

As a highly adaptable social engineering-based attack, phishing rarely encounters technical barriers when adjusting to new environments and work paradigms. It is a threat that can affect customers, vendors, and employees.

Understanding how phishing impacts business brings significant advantages, as combating this threat—mainly through agile and precise takedown efforts—tends to reduce the exposure of a company's brand across a wide range of digital fraud schemes. Since credentials and information stolen via phishing represent a significant risk to corporate networks, the lack of visibility into this threat often complicates identity management.

Security Culture

Policies are ineffective if individuals fail to understand their value. Shadow IT—caused by irregular system provisioning—and errors in identity management, such as retaining active credentials of former employees or third parties, are common signs that a company needs to improve its security culture.

Implementing a successful information security policy becomes more straightforward when employees and decision-makers are aware of the risks and understand the importance of adhering to established guidelines. This culture can be strengthened by a robust security awareness program.

9 AI Advancements Redefining Threat Detection and Response

1 Autonomous Security Systems

→ AI creates systems that detect threats and fix vulnerabilities in real time.

2 Enhanced Behavioral Analytics

→ AI identifies anomalies based on behavioral patterns, improving accuracy over time.

3 Predictive Threat Intelligence

→ Algorithms predict emerging attacks using historical data, enabling proactive defenses.

4 Automation and Data Analysis

→ AI automates the analysis of logs and events, allowing teams to focus on complex investigations.

5 Advanced Anomaly Detection

→ Deep learning identifies unknown or complex threats that traditional methods cannot detect.

6 NLP Integration

→ AI facilitates natural language queries, making threat analysis more accessible.

7 Rapid Incident Response

→ AI reduces response times, quickly containing incidents to minimize damage.

8 Collaboration with Intelligence Sharing

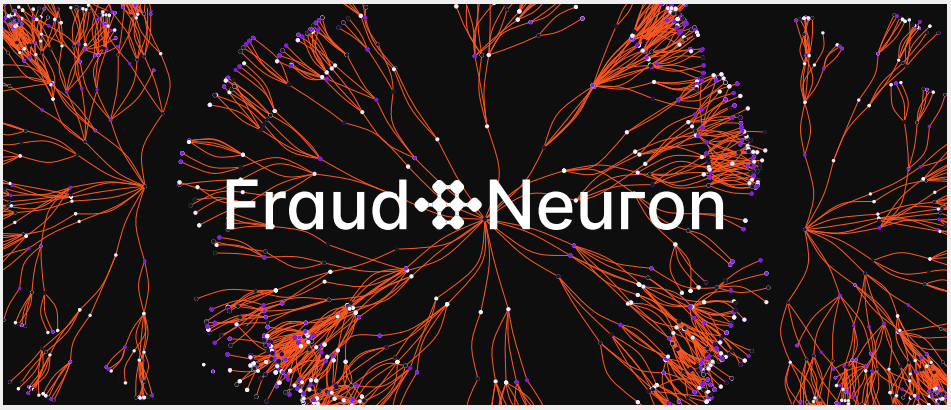
→ AI systems share intelligence in real time, strengthening global security.

9 Focus on Emerging Threats

→ AI tracks threat signals on platforms like social media and dark web forums.

Fraud Neuron

Fraud Modeling Framework



To generate actionable intelligence on cyber threats, they must be described, modeled, and categorized.

The ATT&CK framework, developed and maintained by the MITRE Corporation, is the most established methodology for this purpose, describing an ever-growing list of Tactics, Techniques, and Procedures (TTPs) used by adversaries.

It acts as a common language for cybersecurity professionals to quickly and effectively synthesize and understand attacker behavior, highlighting the critical information defense teams need to detect or prevent a threat.

Each technique is individually cataloged to be referenced within the framework. As a result, ATT&CK functions as both a database and an intelligence repository on the strategies employed by attackers.

Fraud Neuron (F.N.), developed by Axur, aims to fulfill a similar role in the realm of digital fraud, facilitating the exchange of information and creating a shared language for industry professionals.

A Cybersecurity Framework Aligned with Business Needs

By categorizing fraud-specific tactics and their business impacts—including intangible assets such as brand reputation and legal risks—Fraud Neuron complements other modeling approaches and offers a fresh perspective for understanding cybercrime.

Digital fraud blends common elements of cyberattacks with unique attributes tied to the industry in which a company operates, such as e-commerce or financial services. By describing how these combinations occur, Fraud Neuron bridges the gap between cybersecurity and fraud prevention teams, fostering better collaboration.

Open to the Community

Fraud Neuron was developed based on Axur's comprehensive experience in combating digital fraud and has been made available for the entire cybersecurity community. By adopting an open framework, Axur breaks down barriers to information sharing and allows Fraud Neuron to establish itself as a widely recognized language for describing fraud.

Through the project's channels, professionals from any organization can contribute suggestions for improvements or propose new tactics to be included in the model.

Fraud modeling and categorization can also help gather insights about different criminal groups, facilitating quantitative analyses (such as identifying the most common techniques) and serving as a repository of methods used by fraudsters.

The intelligence generated through the Fraud Neuron methodology can be leveraged to prioritize mitigations, design awareness campaigns, and prepare organizations for the types of fraud that most impact their specific industries.

Contribute Fraud Neuron

github.com/axur/FraudNeuron

Core Pillars of Fraud Neuron

→ Target Identification
Type of target (individual or organization)

→ Theme
General category of fraud, including the social engineering theme

→ Reconnaissance
Techniques used to collect data from victims

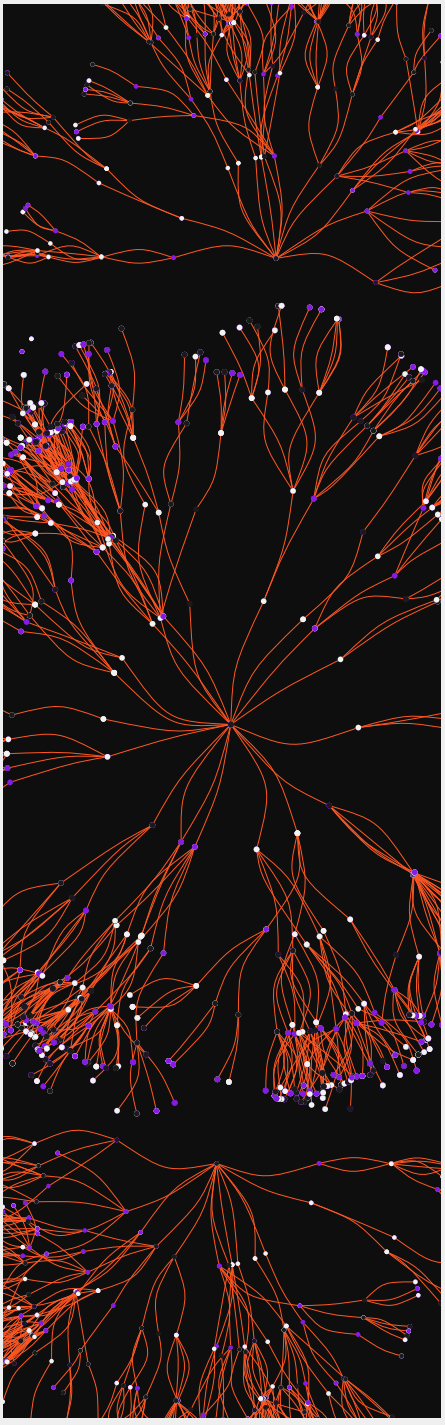
→ Resources
Communication channels, techniques, and tools forming the fraud's digital infrastructure

→ Identity Simulation
Types of identities exploited, such as brands, employees, or applications

→ Social Engineering
Details on how social engineering was applied within the fraud theme

→ Conversion
Techniques for converting a cyberattack into financial gains or other illicit benefits

→ Impact
Business and IT infrastructure impacts associated with the fraud



About Axur

Axur is a leading external cybersecurity solution that empowers security teams to address threats beyond the perimeter. Our platform detects, inspects, and responds to digital fraud, phishing, mentions on the deep & dark web, vulnerabilities, and more.

With automated workflows and the best takedown capabilities in the market, Axur swiftly and efficiently removes malicious content 24/7, managing 86% of detections without human intervention. Our solutions leverage Artificial Intelligence to scale threat intelligence by 180 times, freeing your team to focus on more strategic initiatives.

What security teams are saying about us

Gartner Peer Insights™ 5/5

★★★★★

Exploring the Powerful Partnership with Axur

Axur is our partner, the best one! Even if I need help or have any questions, I call them to help.

IT Security and Risk Management

★★★★★

Intuitive console for efficient configuration of alerts

Speed to identify threats and report them to the customer, with quick and easy implementation.

Technology Manager

Discover how our solutions can transform your security strategy.

Get a Demo

///AXUR

Digital experiences made safe

www.axur.com