SOCRadar®
Your Eyes Beyond

Japan
Threat Landscape Report 2026

Executive Summary **3**
Top Takeaways 3
Technical Details **4**
Dark Web Threats Targeting Japan 5
Industry Distribution of Dark Web Threats 5
Distribution of Dark Web Threats by Threat Categories 6
Distribution of Dark Web Threats by Threat Type 7
Recent Dark Web Activities Targeting Entities in Japan 8
Ransomware Threats Targeting Japan 11
Top Ransomware Groups Targeting Japan 11
A Closer Look into The Top 3 Ransomware Groups 12
Recent Ransomware Attacks Targeting Entities in Japan 15
Phishing Threats Targeting Japan 18
Phishing Attacks - Distribution by Industry 18
Phishing Attacks - Distribution by Phishing Page Title 19
Phishing Attacks - Distribution by SSL/TLS Protocol 20
Strategic Recommendations **21**

Executive Summary

Top Takeaways

- 66.24% of Dark Web threat categories and 33.60% of threat types involve data breach and compromise. Combined with Manufacturing's 40.89% share as the most targeted industry, the primary threat model targeting Japan is industrial data theft, with a focus on intellectual property and supply chain information.

- Manufacturing dominates Dark Web threats at 40.89%, but does not appear in the phishing top ten at all. National Security and International Affairs leads phishing at 19.49%. Dark Web and phishing campaigns target completely different sectors in Japan.

- Qilin alone accounts for 41.5% of ransomware incidents, nearly five times more than the second group, The Gentlemen (8.1%). Japan faces a highly concentrated ransomware threat from a single dominant actor rather than a fragmented landscape.

- 77.6% of phishing sites use HTTPS, making the traditional "look for the padlock" advice ineffective for identifying threats.

- Only 1 out of the top 10 phishing page titles is Japan-specific. The majority of phishing infrastructure uses globally recycled templates in Hebrew, Italian, and English, indicating that Japan is caught in broad multi-country campaigns rather than targeted local operations.

- Banking (14.44%) and Finance (2.89%) together account for 17.33% of phishing, nearly matching Cryptocurrency and NFT (17.33%) on their own. Financial sector phishing is split evenly between traditional banking and digital asset platforms.

- AI-enabled threats rank third in Dark Web categories at 5.44% but drop to 1.99% by threat type. Threat actors are actively discussing AI capabilities, but actual AI-driven attack execution remains low.

- National Security and International Affairs leads phishing (19.49%) while espionage and state-sponsored activity appears in both Dark Web categories (3.99%) and types (1.39%). This pattern points to coordinated intelligence-gathering operations using phishing as the primary entry point.

Technical Details

This report based on data collected between July 2025 and July 2026

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around Japan.

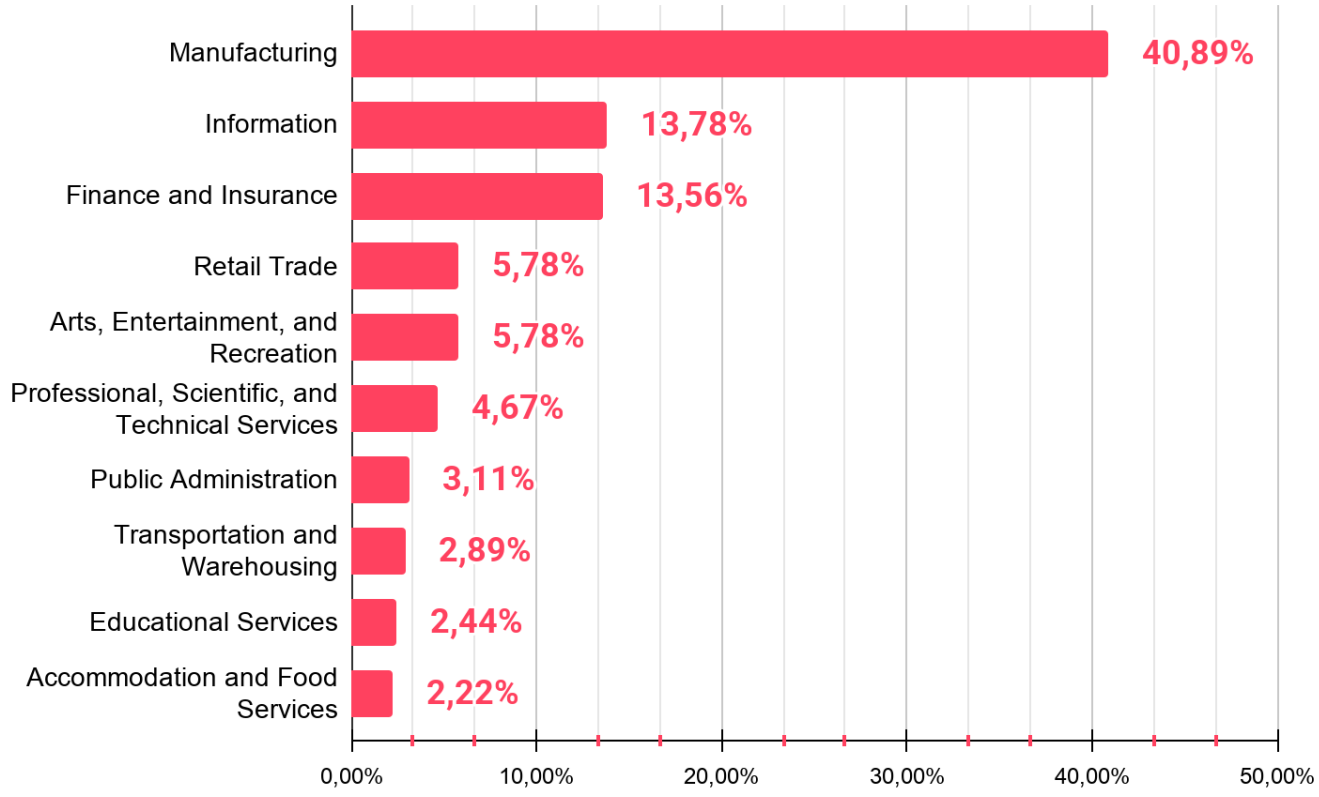
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting Japan, their detailed profiles and the necessary data that summarizes the ransomware activities.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

Dark Web Threats Targeting Japan

Industry Distribution of Dark Web Threats

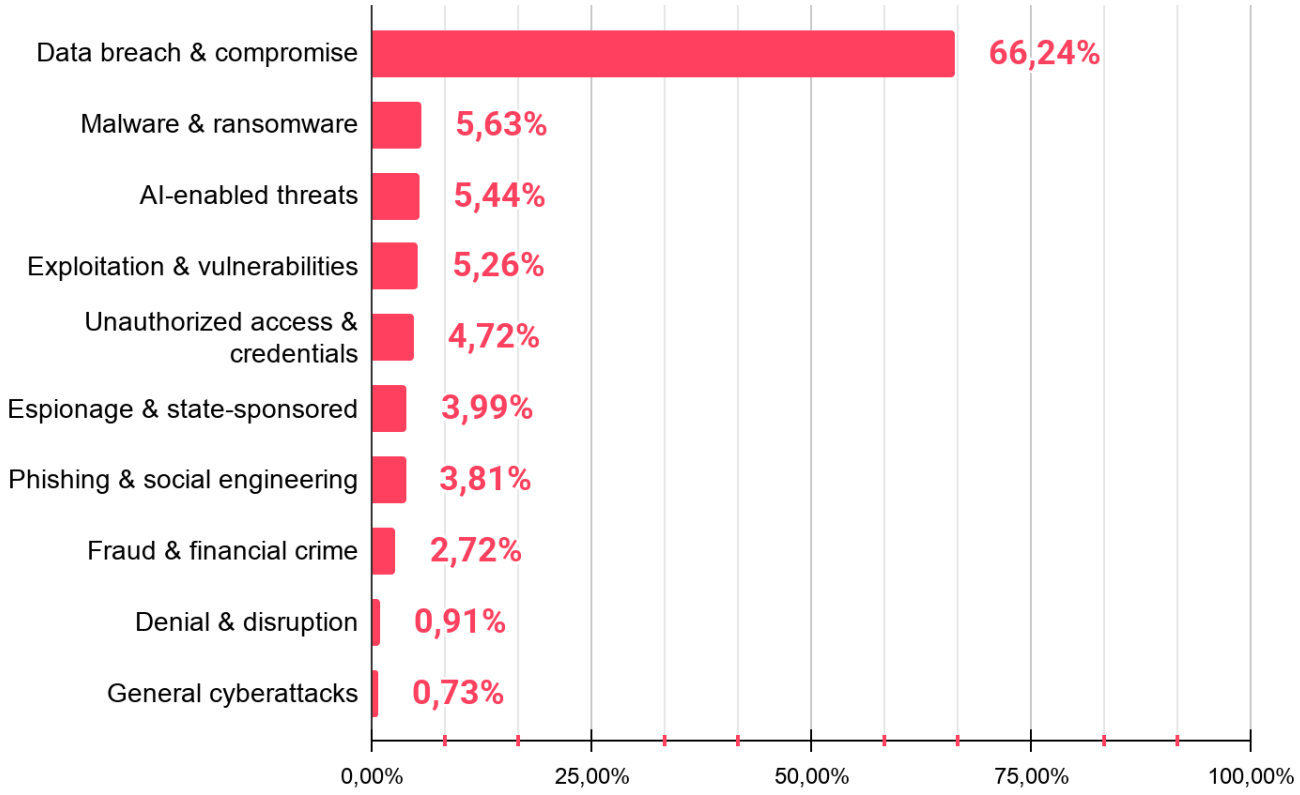


Manufacturing stands out as the most targeted industry in Japan's Dark Web threat landscape, accounting for nearly 41% of all recorded threats. This is roughly three times higher than the next sectors on the list. Japan's position as a global manufacturing hub, home to major automotive, electronics, and industrial companies, makes this sector a high-value target for threat actors looking for proprietary data and supply chain access.

Information (13.78%) and Finance and Insurance (13.56%) follow closely together in second and third place. Both sectors handle large volumes of sensitive data, which makes them attractive for data theft and extortion operations. Together, the top three industries represent over 68% of all Dark Web activity targeting Japan.

The remaining sectors, including Retail, Arts and Entertainment, and Professional Services, each stay below 6%. This concentration at the top shows that threat actors prioritize industries with high-value intellectual property and financial data.

Distribution of Dark Web Threats by Threat Categories

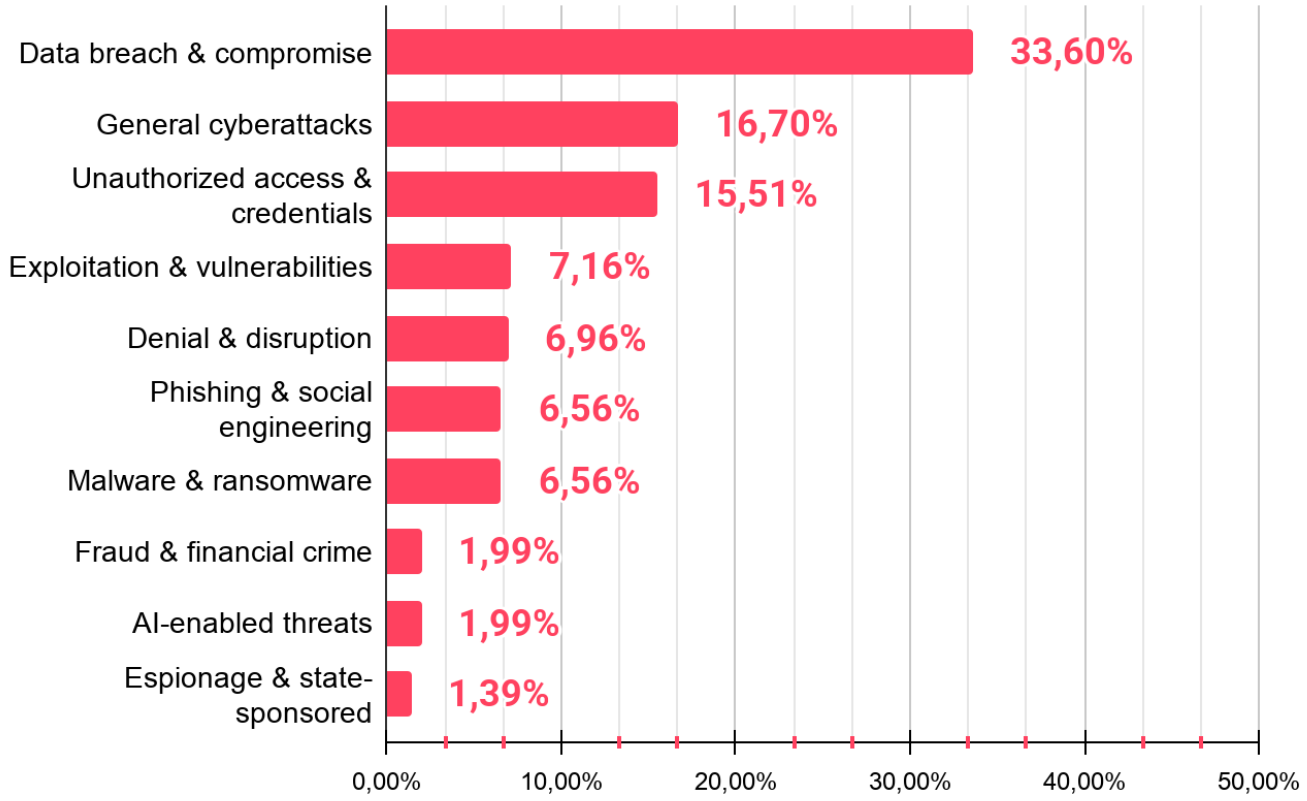


Data breach and compromise is the dominant threat category in Japan, making up 66.24% of all Dark Web activity. This means two out of every three threats involve stolen or exposed data. Given that manufacturing leads the industry distribution, a significant portion of these breaches are tied to intellectual property, trade secrets, and supply chain information from Japan's industrial base.

The next four categories cluster tightly between 4.7% and 5.6%. Malware and ransomware (5.63%), AI-enabled threats (5.44%), exploitation and vulnerabilities (5.26%), and unauthorized access and credentials (4.72%) form a second tier. The presence of AI-enabled threats this high in the ranking signals that threat actors are already adopting AI tools in their operations against Japanese targets.

Espionage and state-sponsored threats account for nearly 4%, which aligns with Japan's strategic importance in technology and defense sectors. Phishing and social engineering remain a consistent entry point at 3.81%.

Distribution of Dark Web Threats by Threat Type



Data breach and compromise remains the leading threat type at 33.60%, but the distribution here is more spread out compared to the category-based breakdown. This shift shows that while data breaches dominate in volume, the actual methods used by threat actors are more diverse.

General cyberattacks (16.70%) and unauthorized access and credentials (15.51%) rank second and third. The high share of unauthorized access threats points to a strong market for stolen credentials and compromised accounts on Dark Web forums targeting Japanese organizations.

Denial and disruption (6.96%), phishing and social engineering (6.56%), and malware and ransomware (6.56%) each hold similar shares, forming a middle tier. Notably, AI-enabled threats drop to 1.99% by type, compared to 5.44% by category. This shows that while AI-related threat discussions are frequent, the actual attack types using AI remain limited in practice.

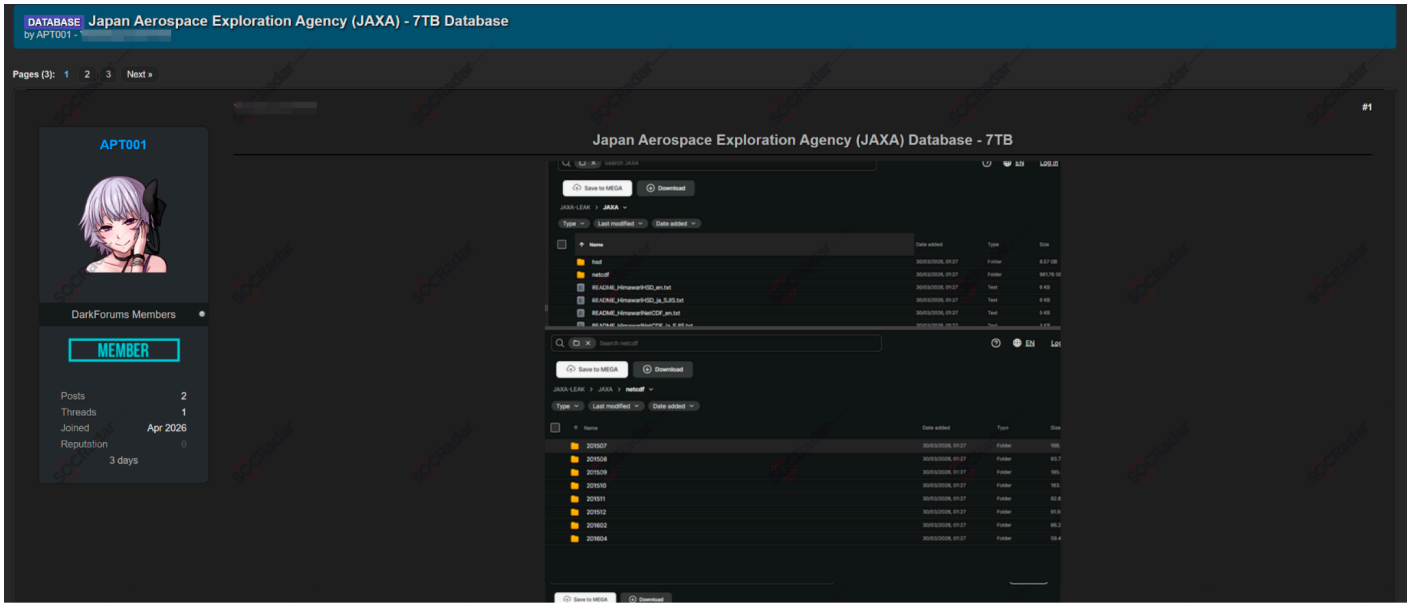
Recent Dark Web Activities Targeting Entities in Japan

Alleged Database of Japan National Tourism Organization Offered for Sale on Hacker Forum

A threat actor is offering a database allegedly belonging to a Japanese government tourism agency on a Dark Web forum. The listing includes sample data containing personal identifiable information. The agency provides tourism promotion and visitor support services across Japan.

Breaches like this can affect both domestic and international individuals whose data was collected through tourism-related services.

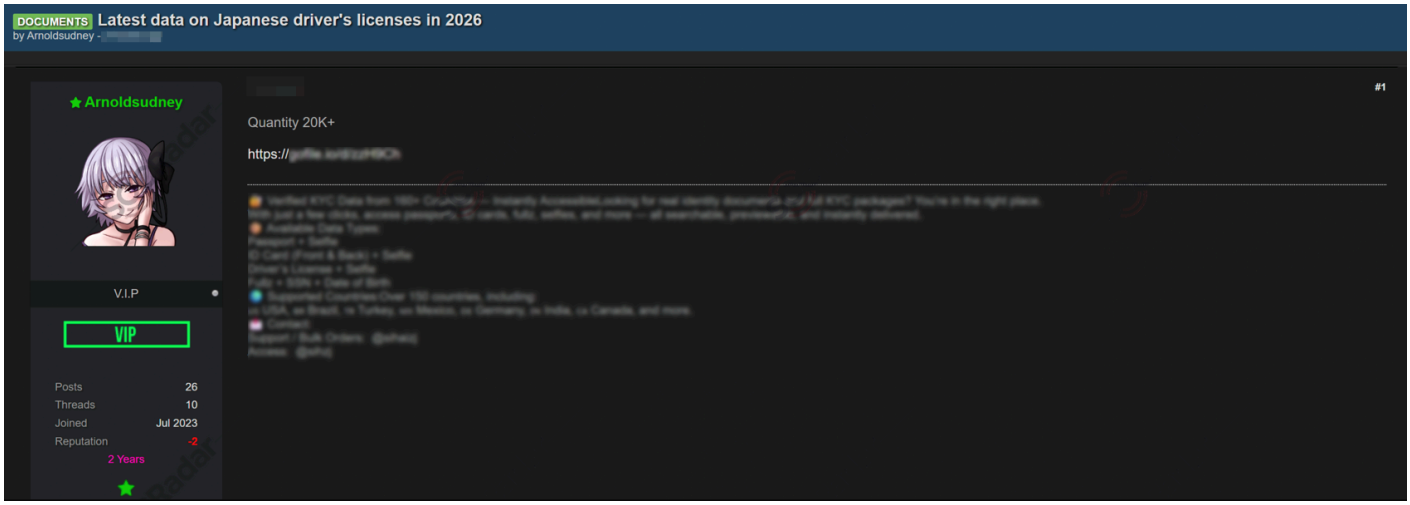
Alleged 7TB Database of Japan Aerospace Exploration Agency (JAXA) Offered for Sale



A threat actor has listed a 7TB database on a Dark Web forum, claiming it was exfiltrated from Japan's national aerospace research agency. The asking price is set at 500 USD.

The agency manages space exploration, satellite development, and advanced aerospace research.

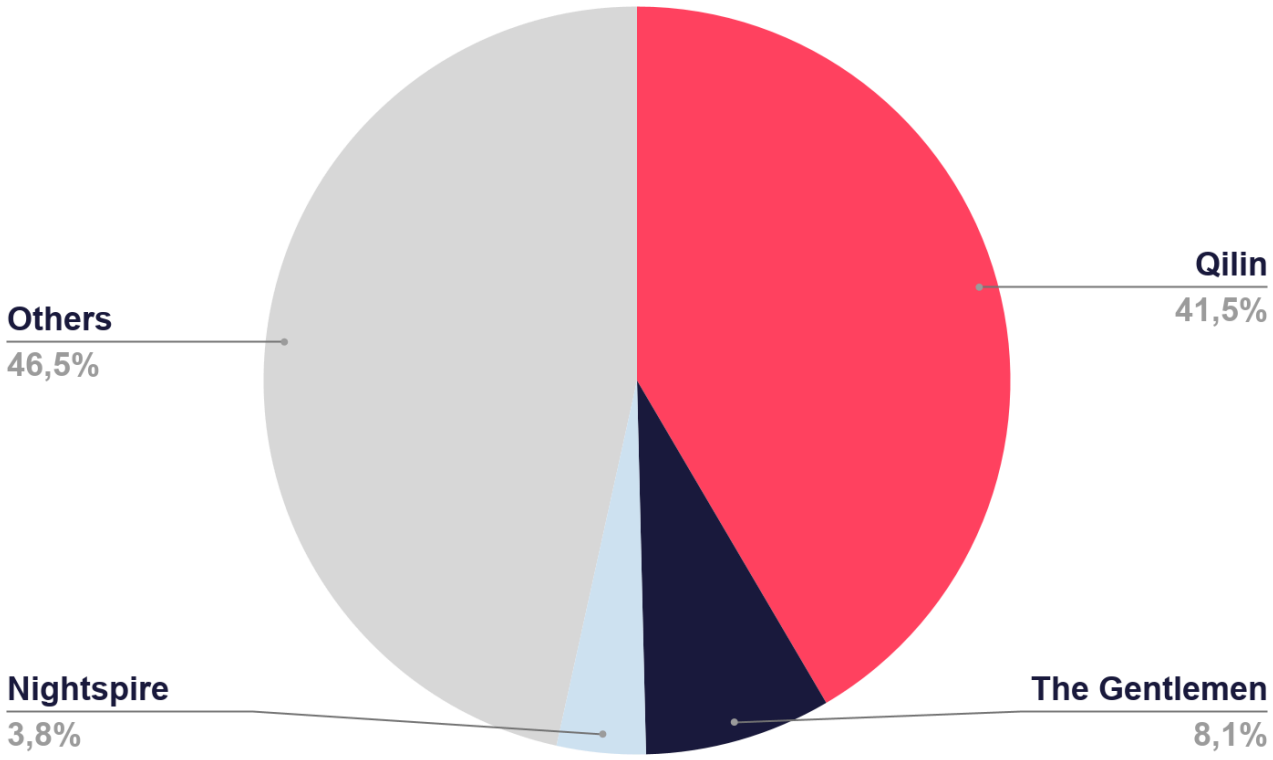
Alleged Leak of 20,000+ Japanese Driver's License Records Surfaces on Dark Web



A threat actor has posted a database on a Dark Web forum claiming to contain over 20,000 Japanese driver's license records. The leaked data reportedly includes personal identification details of license holders. Breaches like this can expose thousands of individuals to identity fraud and document forgery risks.

Ransomware Threats Targeting Japan

Top Ransomware Groups Targeting Japan



Qilin is the most active ransomware group targeting Japan, responsible for 41.5% of all ransomware incidents. This heavy concentration around a single group means that Japan faces a focused and persistent threat from one operation rather than a spread-out risk across many actors.

The second most active group, The Gentlemen Ransomware, accounts for 8.1%, followed by Nightspire Ransomware at 3.8%.

The "Others" category holds 46.5%, indicating that beyond the top three, the ransomware landscape is fragmented across many smaller groups. This creates a dual challenge for defenders: they need to prepare for Qilin's focused campaigns while also maintaining broad defenses against a long tail of less prominent but still active groups.

A Closer Look into The Top 3 Ransomware Groups

Qilin Ransomware

Qilin, also known as Agenda ransomware, represents a formidable threat in cybercrime. This ransomware, one of the known Ransomware-as-a-Service (RaaS) groups, is designed with adaptability in mind, allowing it to customize attacks based on its victims' specific environments. Originating from a sophisticated background, Qilin leverages advanced tactics to extort organizations.

The primary objective of Qilin ransomware is financial gain through extortion. It targets organizations across various sectors, with a particular focus on healthcare and education. These sectors are often chosen due to their reliance on critical data and the generally lower levels of cybersecurity compared to more financially-focused industries. By encrypting essential files and demanding a ransom for their decryption, Qilin aims to create significant operational disruptions, compelling victims to pay the demanded ransom to restore their systems.

You can visit our **blog post** to read the rest of the threat actor profile.

The Gentleman Ransomware

The Gentlemen is an emerging ransomware threat group first observed in mid-to-late 2025. While some indicators suggest development activity as early as July 2025, the ransomware group was first clearly observed in active campaigns beginning in August 2025.

The group operates a double-extortion model. After gaining access to a victim's network, the attackers exfiltrate sensitive data, encrypt systems, and threaten to publish stolen information on Dark Web leak sites if ransom demands are not met. This approach increases pressure by combining operational disruption with reputational and regulatory risk.

Technically, The Gentlemen Ransomware is primarily written in Go, with variants targeting Windows, Linux, and ESXi environments. Execution requires a password parameter, a control mechanism that helps prevent accidental deployment in unintended or analysis environments. This design choice reflects a deliberate, operator-driven deployment model rather than indiscriminate spreading.

You can visit our **blog post** to read the rest of the threat actor profile.

NightSpire Ransomware

NightSpire, a financially driven ransomware group, surfaced in early 2025, focusing on small to medium-sized enterprises across multiple industries for opportunistic exploitation. Initially centered on data theft and extortion, the group has shifted to a double extortion strategy, encrypting data after exfiltration, as seen in recent incidents.

NightSpire's operations are global in scope. The group does not appear to focus on a specific country or region, instead choosing victims based on exposed vulnerabilities and a lack of cyber hygiene. The United States is the most targeted country, followed by Taiwan, Hong Kong, Egypt, and several European nations. Other affected countries include India, Japan, France, Spain, and Poland. The geographical spread suggests a non-geopolitical motive, with a primary focus on financially motivated attacks against soft targets.

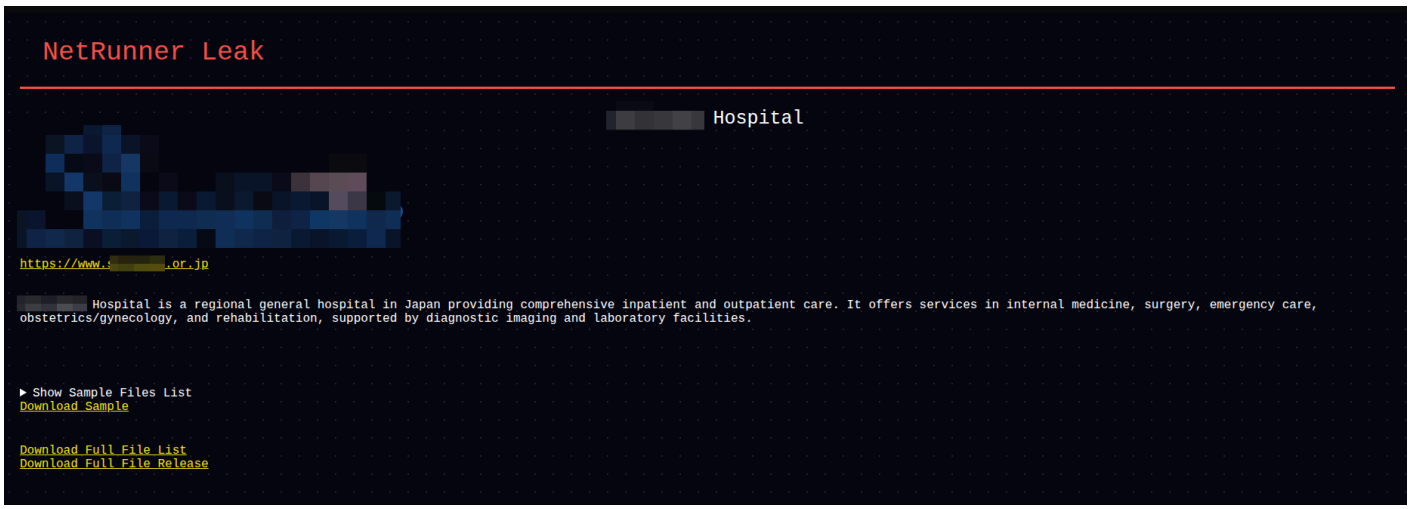
You can visit our **blog post** to read the rest of the threat actor profile.

Recent Ransomware Attacks Targeting Entities in Japan

Qilin Ransomware Group Claims Attack on a Major Japanese Automotive Parts Manufacturer

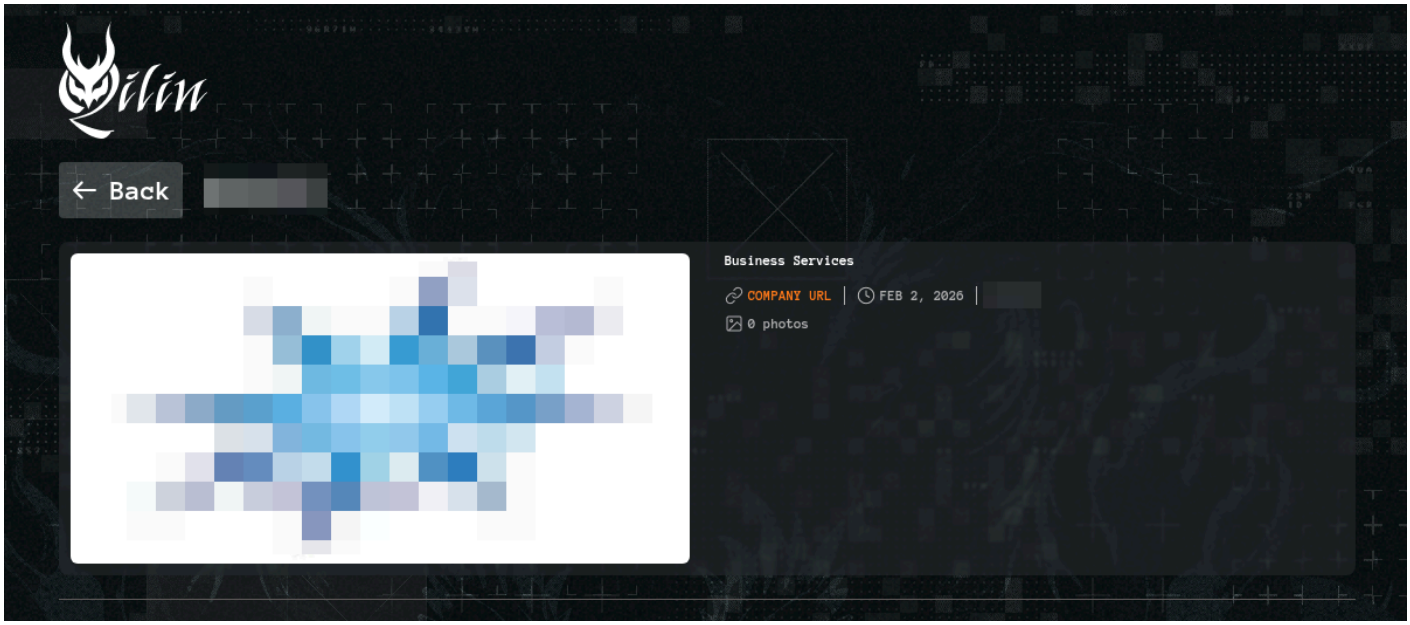
The Qilin ransomware group has added a major Japanese automotive parts manufacturer to its leak site. The targeted company is a key supplier in the global automotive supply chain, providing components to multiple major car manufacturers.

Netrunner Ransomware Group Claims Attack on a Japanese Regional Hospital

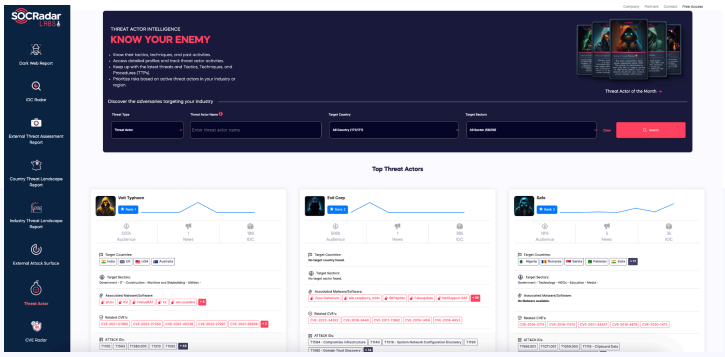


The Netrunner ransomware group has listed a Japanese regional hospital on its leak site, claiming a successful breach. The facility provides essential medical care services to its local community.

Qilin Ransomware Group Claims Attack on a Japanese Specialty Metal Manufacturer



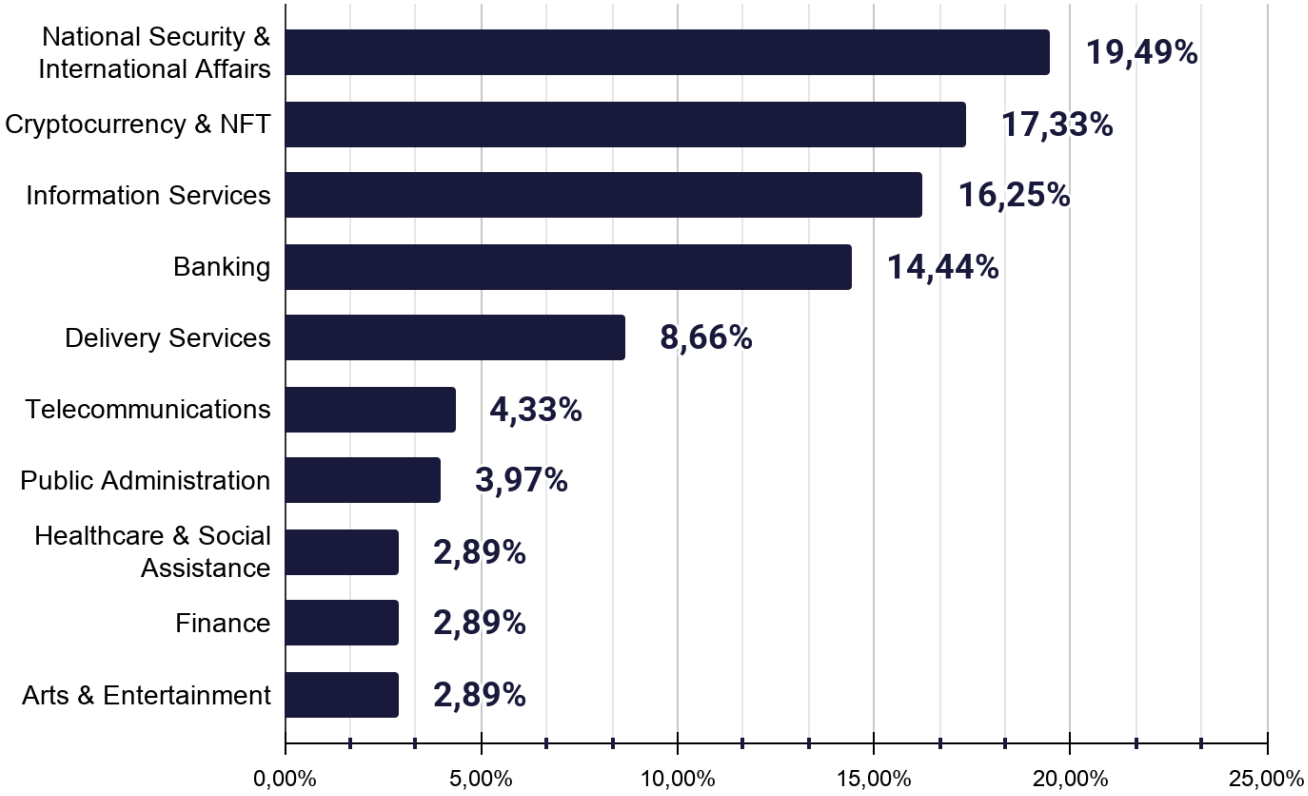
The Qilin ransomware group has listed a Japanese specialty metal manufacturing company on its leak site. The company produces nickel alloy materials, processed components, and plant equipment for industries including batteries, energy, semiconductors, and aerospace.



*SOCRadar enhances cybersecurity measures with its **Threat Actor Intelligence Module**, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.*

Phishing Threats Targeting Japan

Phishing Attacks - Distribution by Industry

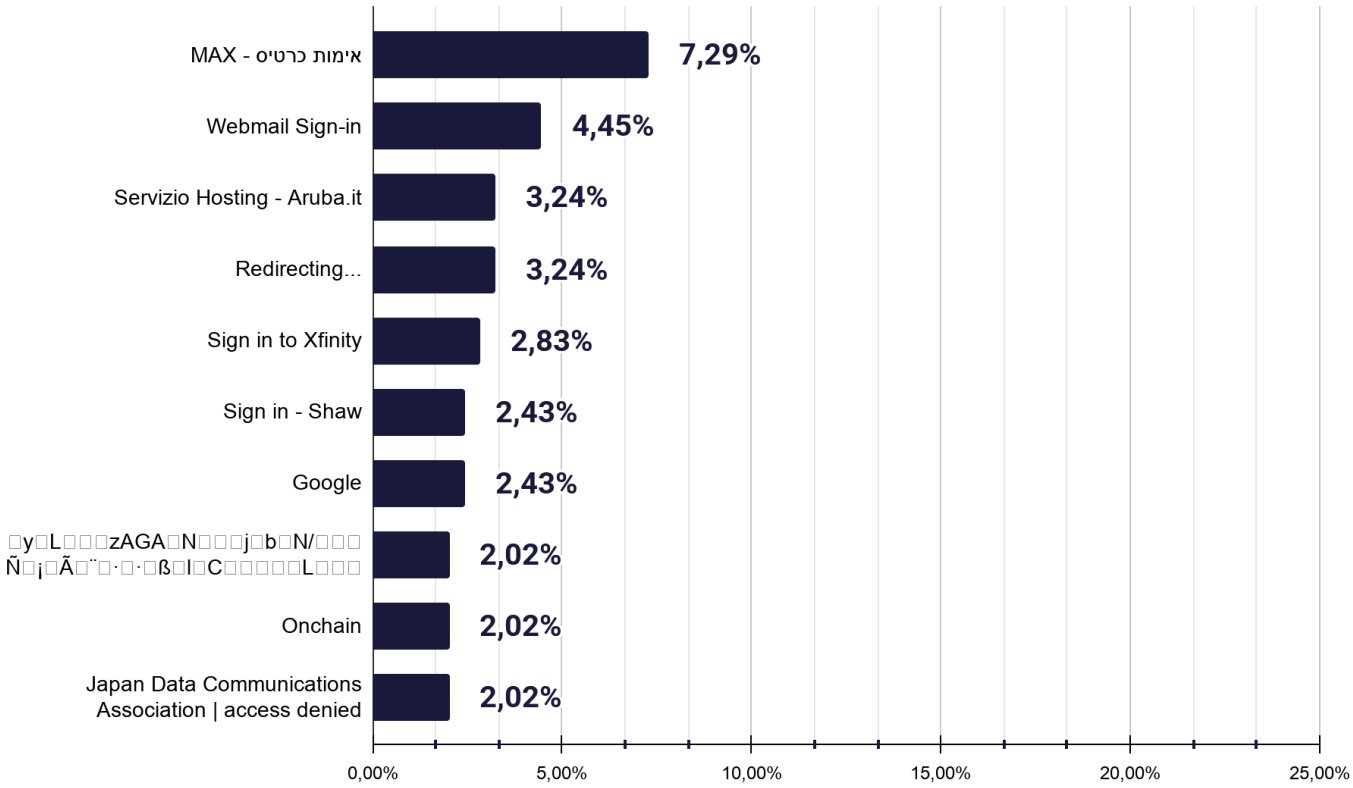


The phishing landscape in Japan shows a very different pattern from the overall Dark Web threat distribution. While manufacturing dominates the broader threat picture, it does not appear in the phishing top ten at all. Instead, National Security and International Affairs leads at 19.49%, which connects directly to the espionage and state-sponsored activity seen in earlier data. Phishing serves as a primary tool for intelligence-gathering operations against government and defense-related targets.

Cryptocurrency and NFT (17.33%), Information Services (16.25%), and Banking (14.44%) follow closely. The top four sectors sit within a narrow 5-point range, showing that phishing efforts are more evenly distributed than other threat types. When Banking and Finance (2.89%) are combined, the financial sector reaches over 17%, matching the cryptocurrency segment.

Delivery Services at 8.66% reflects a Japan-specific trend where fake delivery notification messages are widely used to harvest credentials from individual users.

Phishing Attacks - Distribution by Phishing Page Title

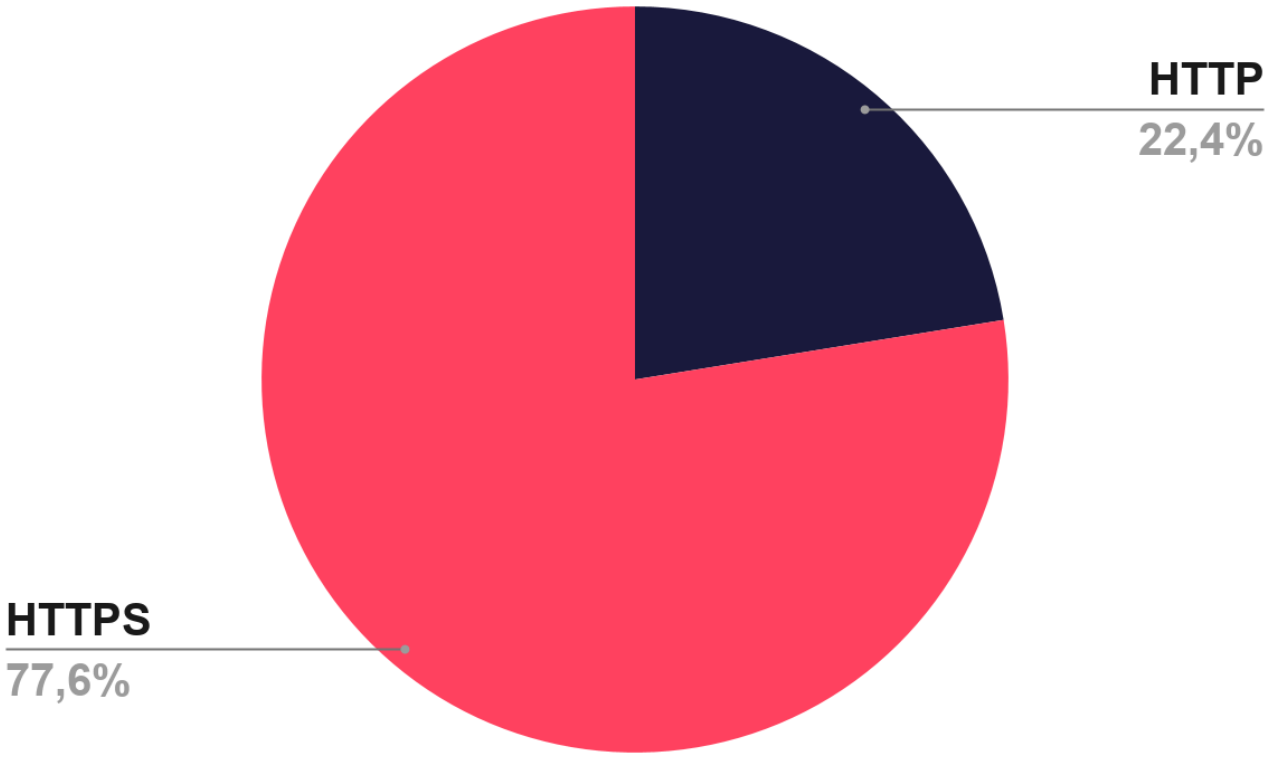


The phishing page title distribution reveals that most campaigns targeting Japan rely on globally recycled phishing infrastructure rather than locally crafted pages. The top entry, a Hebrew-language credit card verification page (MAX), accounts for 7.29%, followed by generic Webmail Sign-in (4.45%) and an Italian hosting service page (3.24%). These are not Japan-specific templates, which indicates that attackers are running broad, multi-country phishing operations that happen to catch Japanese targets.

Only one entry in the top ten is Japan-specific: Japan Data Communications Association (2.02%). The low presence of Japanese-language pages shows that targeted, localized phishing campaigns are either fewer in number or better distributed across unique page titles.

The garbled text entry (2.02%) points to obfuscation techniques used to evade detection systems. Onchain (2.02%) ties back to the high share of cryptocurrency-related phishing seen in the industry breakdown, confirming that crypto platforms remain an active phishing target.

Phishing Attacks - Distribution by SSL/TLS Protocol



Over three-quarters of phishing pages targeting Japan use HTTPS (77.6%), while only 22.4% rely on plain HTTP. This confirms that the old advice of "check for the padlock icon" is no longer a reliable way to identify phishing sites.

The 22.4% still running on HTTP is worth noting. These unencrypted pages are easier for browsers and security tools to flag, which means they have shorter lifespans. Their continued use shows low-effort, high-volume campaigns where attackers prioritize speed over sophistication. This aligns with the earlier finding that many phishing pages use recycled, non-localized templates rather than carefully crafted Japan-specific content.

For Japanese organizations, this data reinforces that HTTPS alone cannot be treated as a trust signal. Security awareness training needs to move beyond basic URL checks toward more advanced verification methods.

Strategic Recommendations

- **Enhance Endpoint Security:** Implement advanced anti-malware, regular device audits, and employee training on safe browsing practices.
- **Strengthen Phishing Defense:** Invest in phishing detection systems, web filtering tools, and employee training on recognizing phishing attempts.
- **Enforce Multi-Factor Authentication (MFA):** Apply MFA across critical systems to protect against stolen credentials.
- **Fortify Ransomware Defenses:** Regularly back up data, segment networks, and develop incident response plans for ransomware attacks.
- **Monitor Dark Web Activity:** Use Dark Web monitoring to detect exposed company data early and respond quickly to breaches.
- **Collaborate on Cyber Threat Intelligence:** Share insights with industry peers and stay informed about emerging threats and new attack vectors.
- **Secure Communications and Data:** Ensure encryption for sensitive communications and transactions, and train employees on secure data handling.
- **Proactive Vulnerability Management:** Regularly apply patches and conduct penetration testing to address potential system vulnerabilities.
- **Build a Cybersecurity Culture:** Foster ongoing employee training, phishing simulations, and establish clear security policies to ensure a security-first mindset across the organization.

How can SOCRadar help your organization?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: "Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services." SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Start free trial

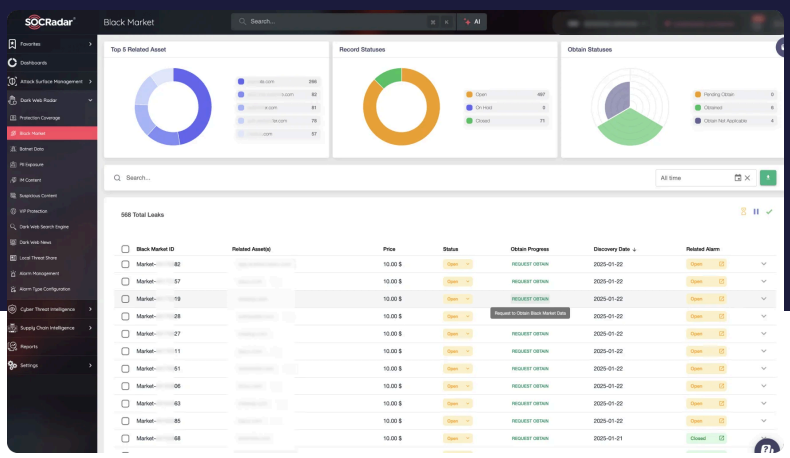
Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.



SOCRadar®
Your Eyes Beyond