MALAYSIA

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Executive Summary

Top Takeaways

- Public Administration is the primary dark web exposure point in Malaysia, representing over 24 percent of observed activity. This makes government related data and access the most attractive targets in the country.

- Dark web threats are highly local. Around 80 percent of general threats and 98 percent of ransomware incidents target Malaysia only, showing limited regional spillover and strong domestic focus.

- Data theft drives the threat landscape. More than 75 percent of dark web threats involve data or databases, while access sales account for another 20 percent, supporting follow on attacks.

- Ransomware activity is fragmented. No single group dominates, and over 60 percent of cases come from smaller or less established actors, increasing unpredictability.

- Phishing focuses on finance and trusted brands. Finance leads with nearly 32 percent, while Booking.com impersonation alone accounts for over 40 percent of phishing page titles.

Technical Details

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

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

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.

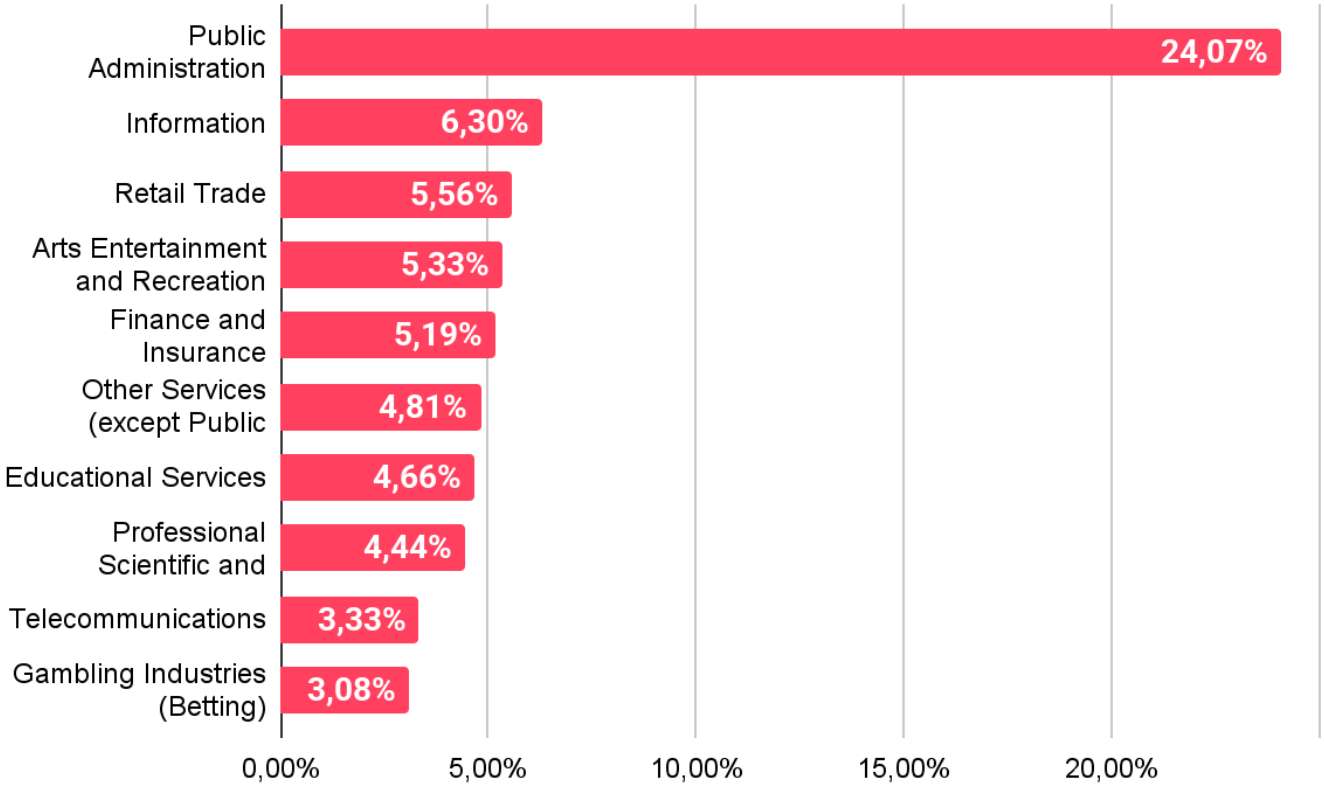
In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting Malaysia, their detailed profiles and the necessary data that summarizes the ransomware activities.

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.

And lastly, the DDoS Attack Statistics shows you the latest information about the intensity of DDoS attacks and how threat actors target organizations to disrupt their operations.

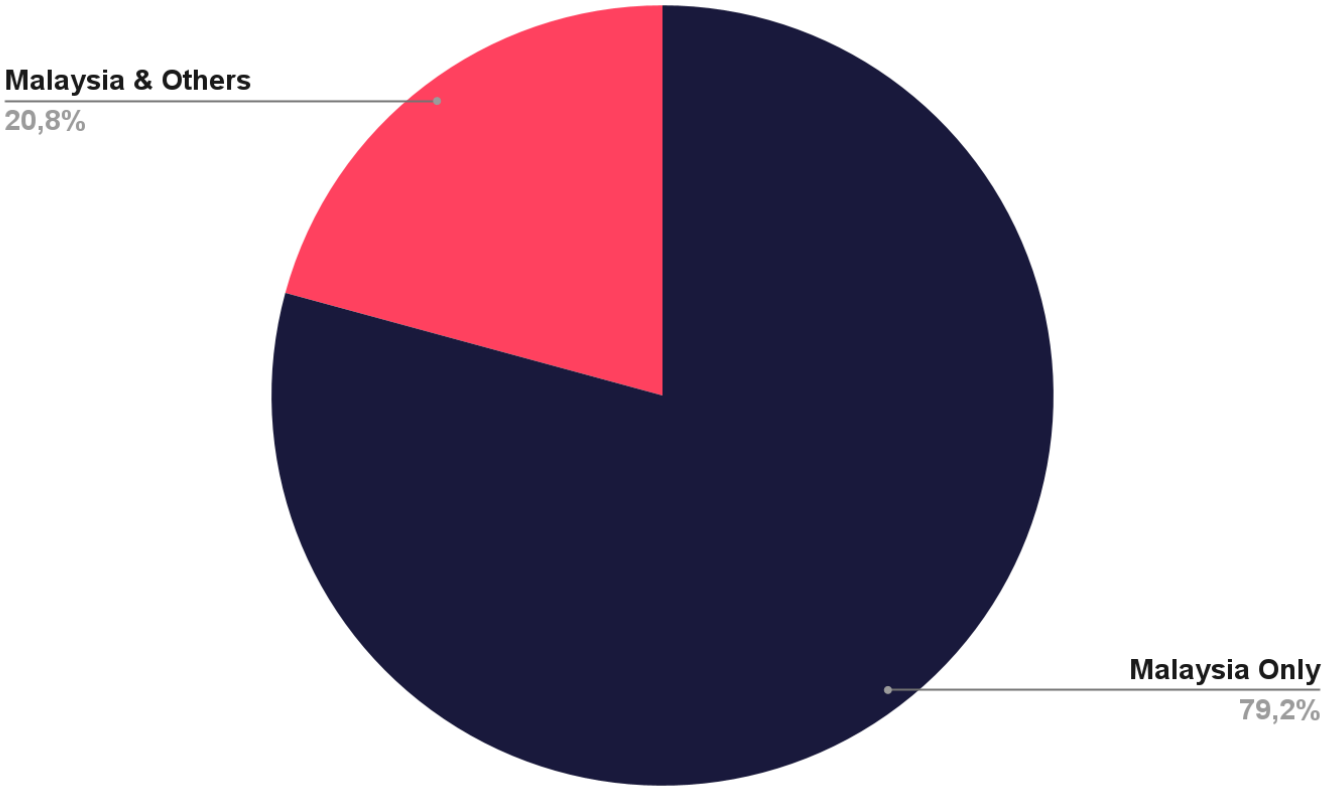
Dark Web Threats Targeting Malaysia

Distribution of Dark Web Threats by Industry



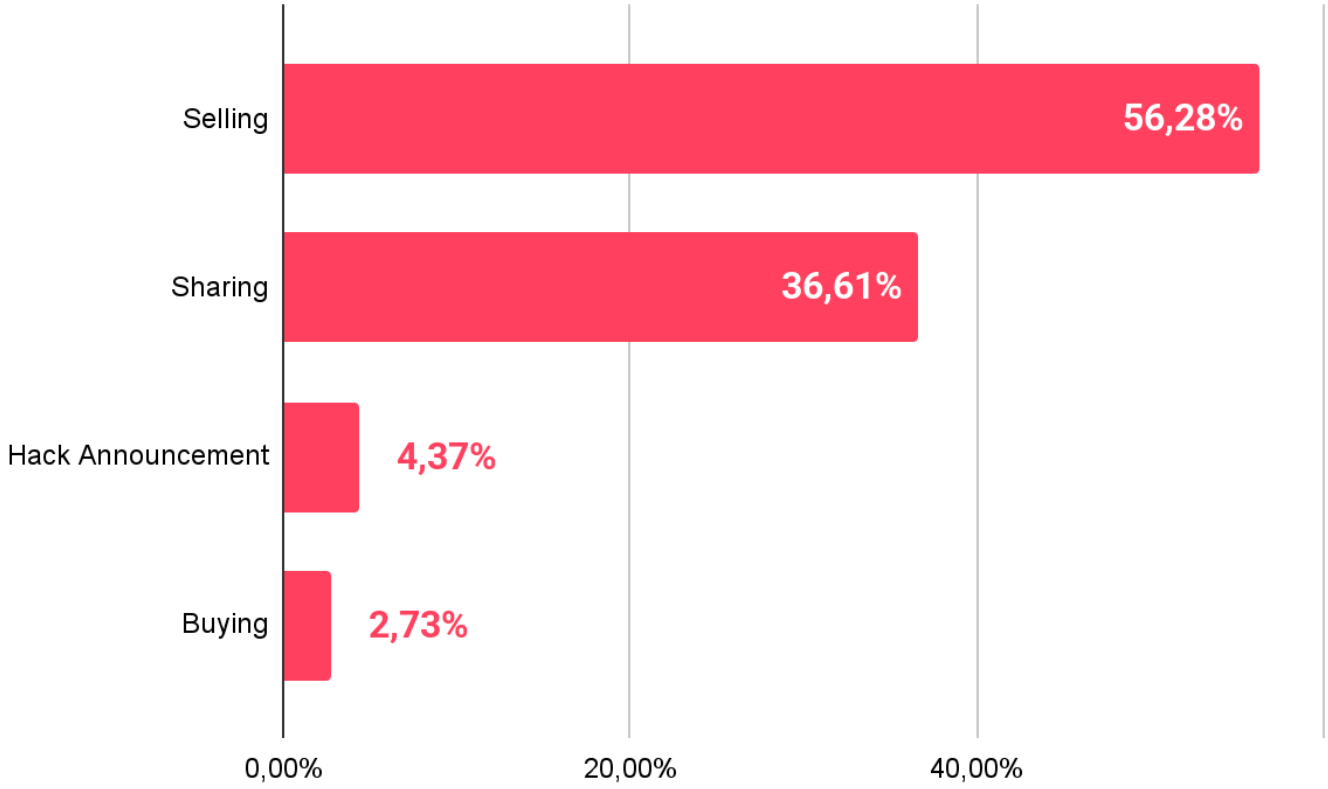
Public Administration dominates dark web exposure in Malaysia with over 24 percent of observed activity. This gap is large compared to other sectors and suggests sustained interest in government related data and access. The Information and Retail Trade sectors follow but remain far behind, each below seven percent. Finance and Insurance appears in the top five, which aligns with its high value for fraud and monetization, even if its share is moderate. Telecommunications and Gambling also show presence, which may support phishing, scams, or illegal services. Overall, threat activity is concentrated on sectors that hold sensitive data or enable downstream criminal operations.

Distribution of Dark Web Threats by Primary Target Country



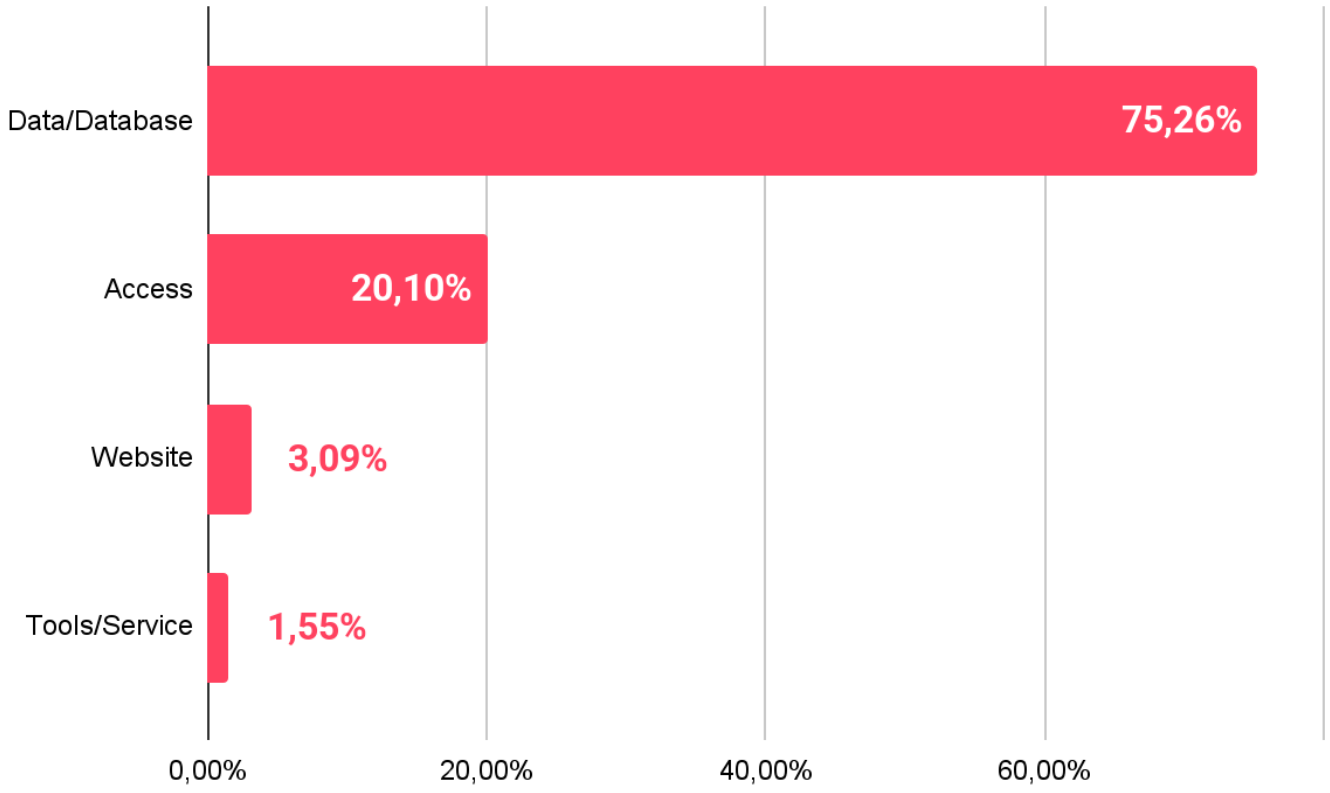
Most dark web threats linked to Malaysia are country specific. Nearly 80 percent of observed activity targets Malaysian entities only, which indicates a strong local focus by threat actors. This may reflect the use of local language, regional knowledge, or domestic data sources. Cross border activity exists but remains limited at around 21 percent. This gap suggests that many campaigns are designed for local impact rather than regional scale. The pattern points to threats that are tailored to national institutions, local businesses, and Malaysian users, instead of broad international operations.

Distribution of Dark Web Threats by Threat Categories



Selling dominates dark web activity linked to Malaysia with over 56 percent of observed threats. This shows that most incidents aim at direct profit through data, access, or services. Sharing follows with more than 36 percent, which suggests active circulation of leaked data and reused content across forums. Hack announcements remain low, which may indicate that many actors prefer silent monetization instead of public claims. Buying activity is minimal and shows limited demand side visibility. Overall, the distribution points to a mature underground market where stolen assets are quickly sold or redistributed rather than openly promoted.

Distribution of Dark Web Threats by Threat Type



Data and database related threats account for more than 75 percent of dark web activity tied to Malaysia. This shows a strong focus on stealing and trading structured data, such as customer records or internal datasets. Access related threats follow at 20 percent, which often support later data theft or fraud operations. Website related threats are limited, suggesting that defacement or simple site abuse is not a main goal. Tools and services appear rarely and indicate low visibility of local threat tooling. Overall, the data confirms that information theft remains the primary driver of dark web activity.

Recent Dark Web Activities Targeting Entities in Malaysia

Alleged Database of Malaysia Aviation is on Sale

In a Dark Web forum monitored by SOCRadar, an alleged database sale has been detected involving a major airline operating in Malaysia.

The dataset is advertised as a 490 MB text dump containing approximately 1.06 million records from 2025. The exposed data reportedly includes passenger travel and identity information such as full names, dates of birth, gender, phone numbers, booking IDs, email or loyalty login identifiers, nationality, and partial passport details with issuing countries.

The presence of booking identifiers and verified personal attributes suggests a risk of passenger profiling, identity misuse, and abuse of airline loyalty or ticketing systems.

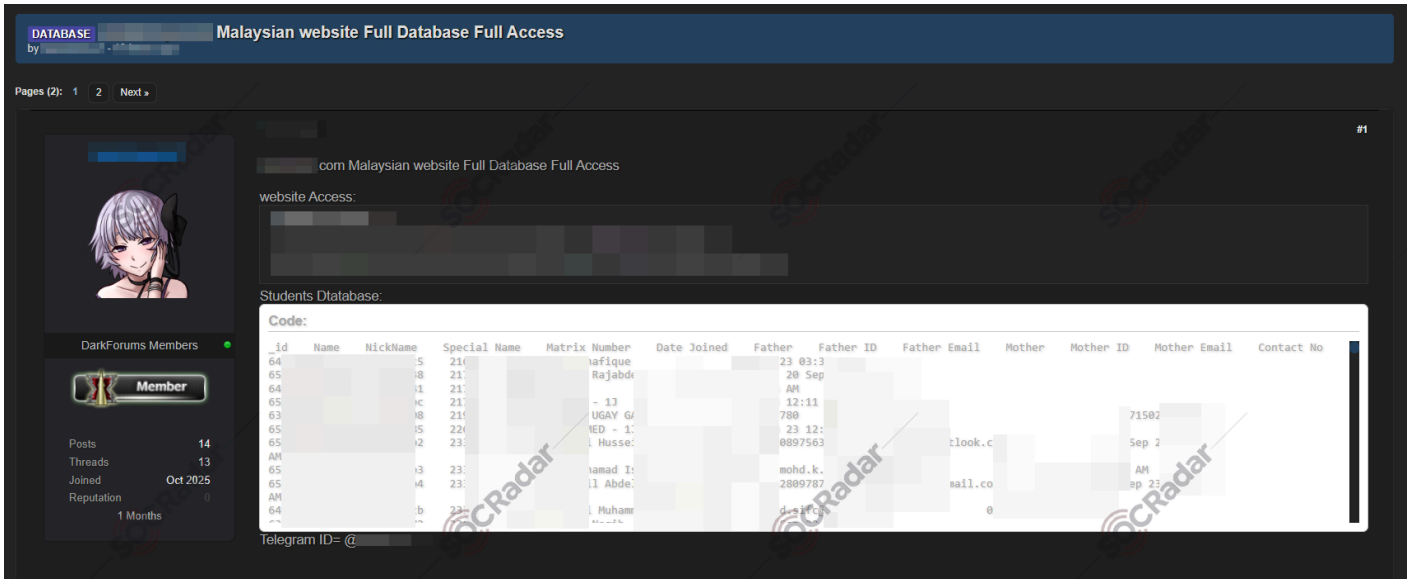
Alleged Blueprints and Documents for Malaysian Navy are on Sale

In a Dark Web forum monitored by SOCRadar, a threat actor claims to be selling sensitive documents allegedly related to a naval technology company, working on navigation, imaging and positioning solutions, and its work with the Malaysian Navy.

The post advertises blueprints and internal documents for sale, with pricing in the five-figure range and negotiations offered. The seller claims to provide samples and requests proof of funds before sharing the full file list.

Leaked technical documents may expose military capabilities and design weaknesses. The data could support espionage, countermeasure development, or supply chain targeting.

The Alleged Unauthorized Access and Database of an Education Platform are Leaked



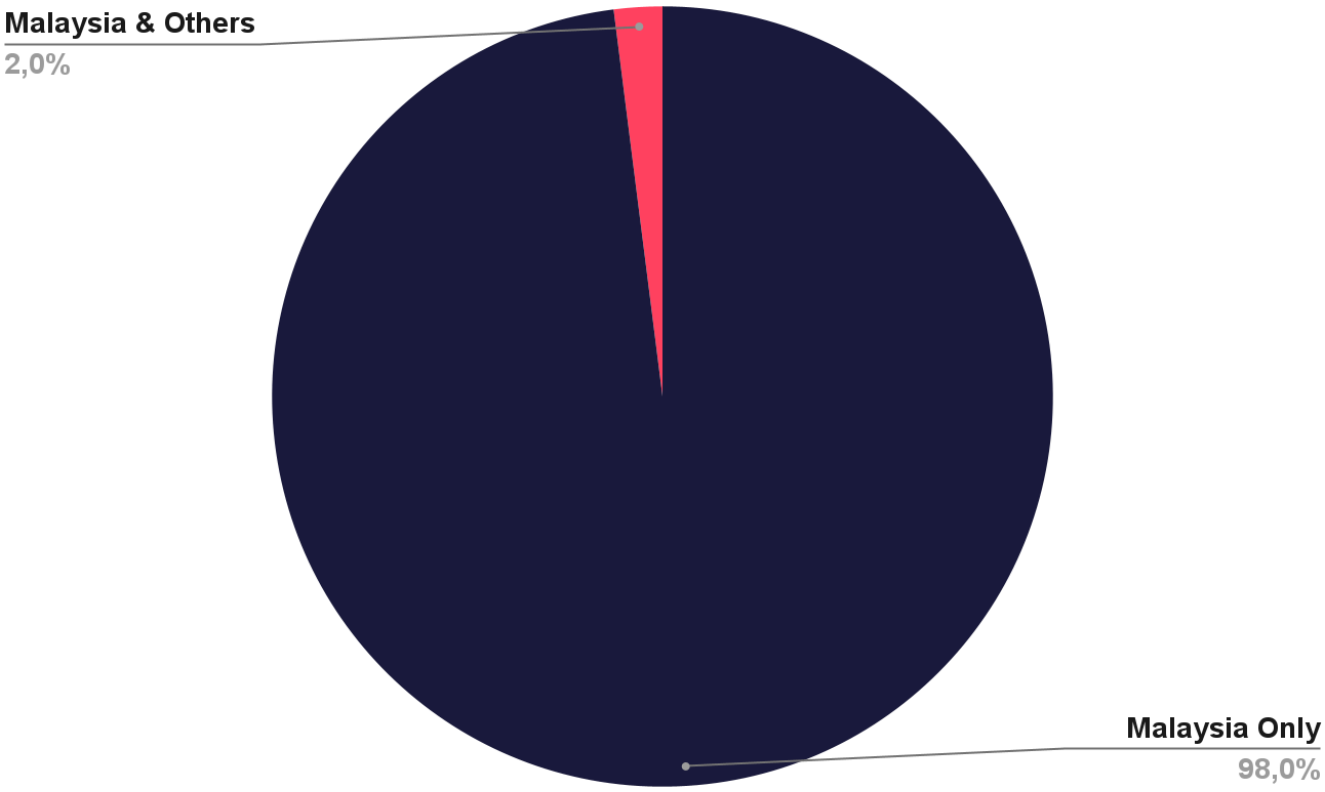
In a Dark Web forum monitored by SOCRadar, a threat actor claims to be selling unauthorized access and a full database dump allegedly belonging to a Malaysia-based education app.

The post advertises full website access along with a student database containing personal and family-related information, including names, matriculation numbers, contact details, and parents' identities and email addresses. The app helps schools track attendance, reward positive behaviour, and manage students more efficiently.

Exposed student and parent data can enable phishing, scams, and identity misuse. Enrollment and ID details may be abused for account takeover and long term profiling.

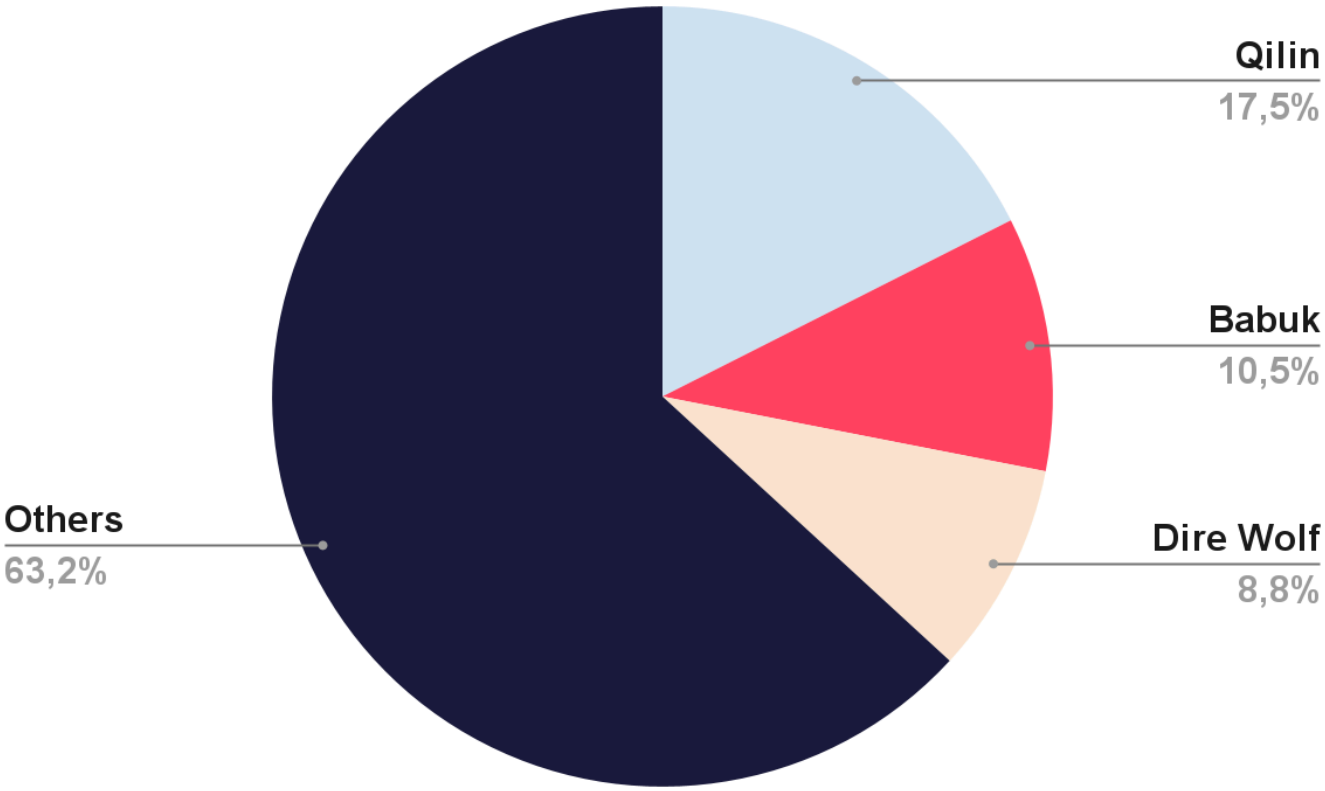
Ransomware Threats Targeting Malaysia

Distribution of Ransomware Attacks by Primary Target Country



Ransomware threats linked to Malaysia are almost fully domestic in scope. About 98 percent of observed cases target Malaysian organizations only. This shows a very strong local focus by ransomware actors. Such targeting often relies on local exposure, known vulnerabilities, or limited security maturity within specific sectors. Cross border ransomware activity is almost absent, which suggests Malaysia is not commonly used as part of regional campaigns. Instead, actors appear to select Malaysian victims directly and operate within national boundaries. This pattern increases the importance of local detection, response, and coordination rather than regional threat sharing alone.

Top Ransomware Groups Targeting Malaysia



Ransomware activity in Malaysia is fragmented across many actors. Qilin leads among named groups but accounts for less than one fifth of observed cases. Babuk and Dire Wolf follow with lower and close values, which shows no single dominant operator. The large share attributed to other groups suggests frequent involvement of smaller or short lived ransomware crews. This pattern points to an unstable threat environment where targets face varied tactics and tooling. It also suggests that Malaysia is part of a broader opportunistic ransomware landscape rather than a focus of one major campaign.

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.

Babuk/Babuk2 Ransomware

Babuk, originally emerging in 2020, became infamous for its ransomware attacks on large organizations and government agencies. After internal conflicts led to the leak of its source code, the group disbanded, giving rise to Babuk V2, which shifted to data theft and extortion.

In 2025, a new iteration, Babuk2, resurfaced under the alias Bjorka, a notorious hacker known for targeting the Indonesian government. While claiming massive data breaches and extortion, Babuk2's true capabilities are unclear, with many of its leaks seeming to be recycled from previous incidents. Despite doubts, Babuk2 continues to capitalize on fear and reputation, pushing its ransomware operation for profit.

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

Dire Wolf Ransomware

Dire Wolf emerged in 2025 and quickly carried out disruptive ransomware attacks in multiple regions. They present themselves with a blunt message on its leak site: “We only seek money. No morals, no political stance.” The statement is intended to intimidate victims and to emphasize a purely financial motive.

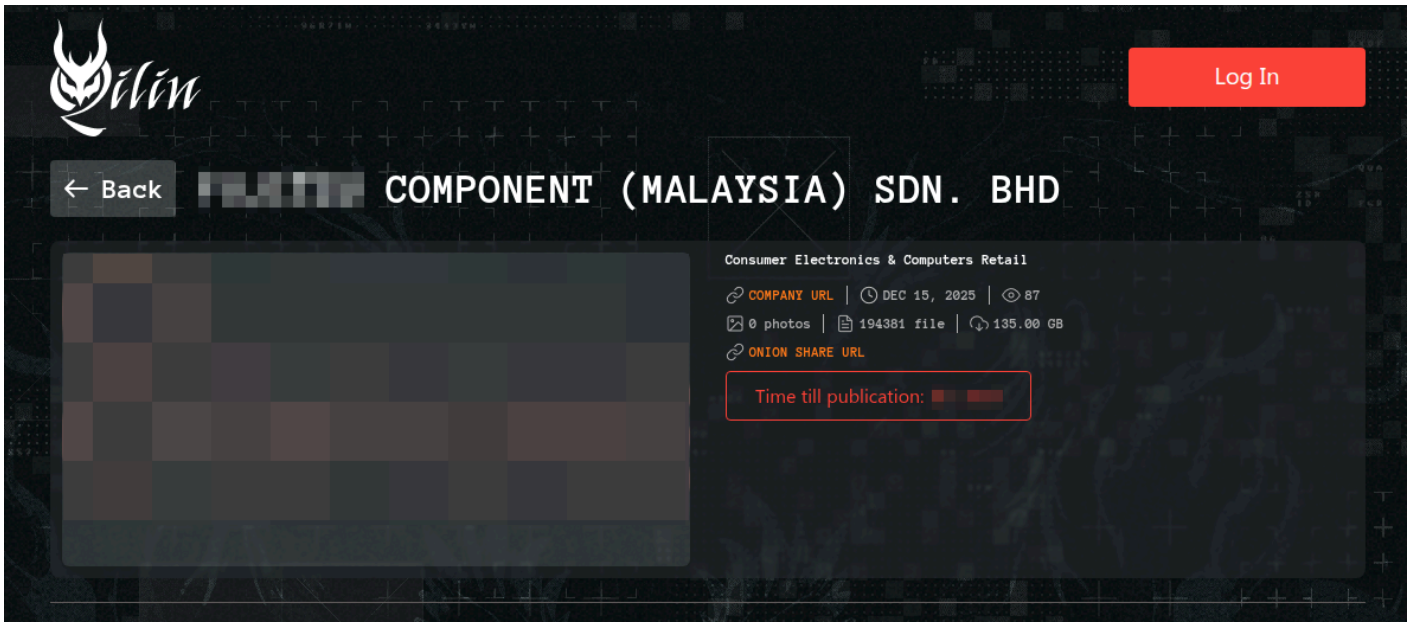
In just a few months, the group claimed responsibility for 41 victims worldwide. Early disclosures highlighted organizations in Thailand, Taiwan, Singapore, and the United States among the most impacted.

The operators run a classic double extortion model. They steal data, encrypt systems, then threaten publication on a Tor leak site if talks fail.

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

Recent Ransomware Attacks Targeting Entities in Malaysia

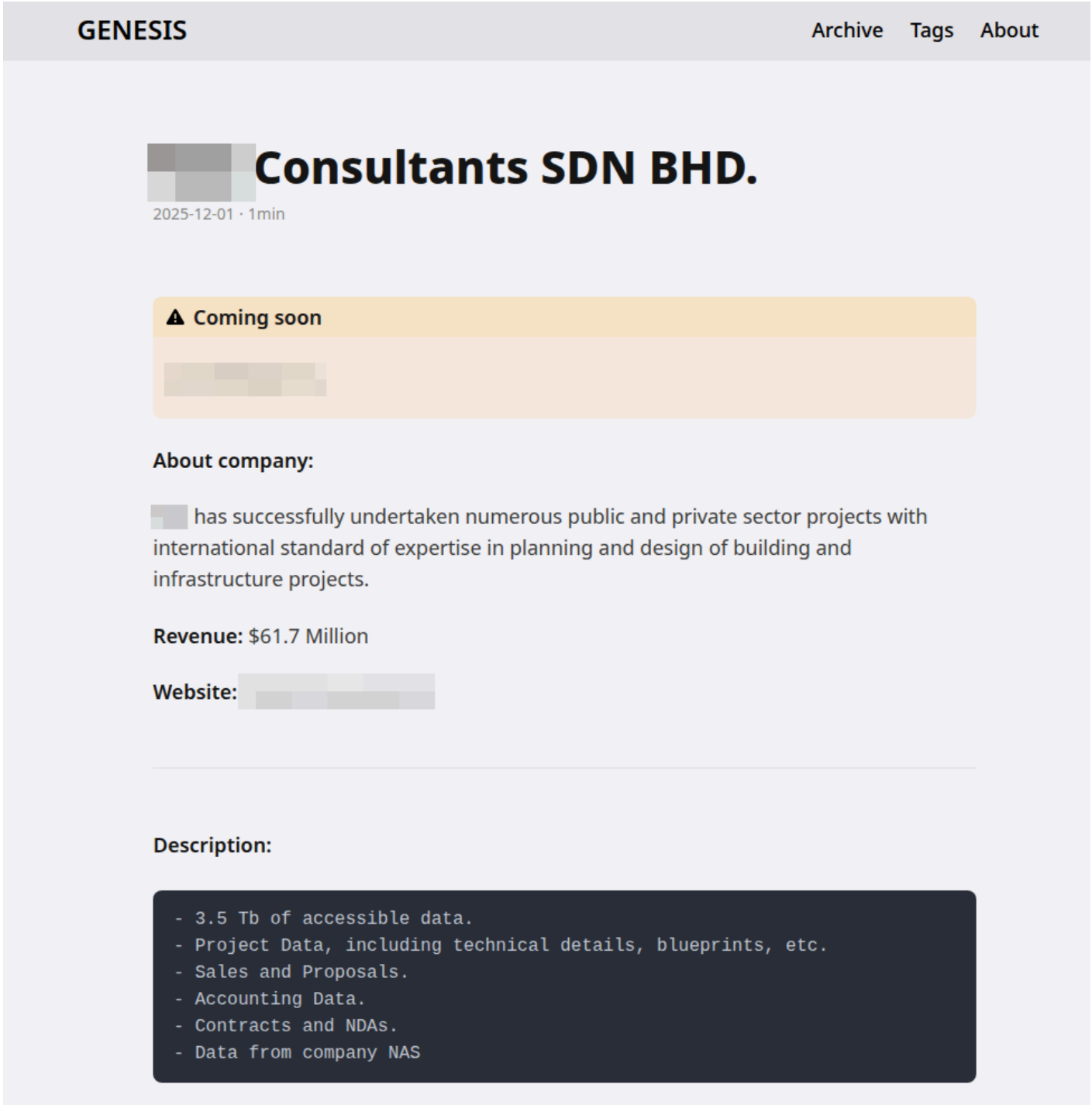
Malaysia Electronics Manufacturer Listed on Qilin Ransomware Leak Site



In the Qilin ransomware group leak site monitored by SOCRadar, a new ransomware victim was listed from the electronics manufacturing sector in Malaysia.

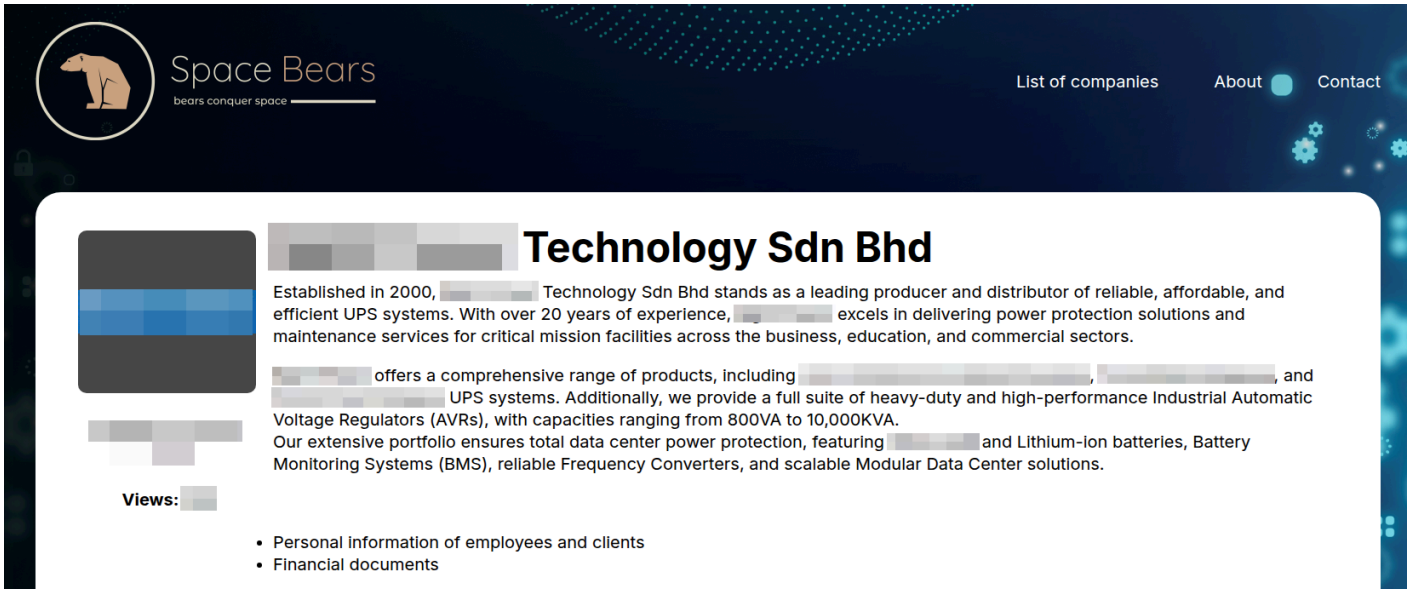
The affected organization operates in the production of electronic and electromechanical components, supplying parts used in automotive systems, industrial equipment, and information and communication technology hardware. Its services include component manufacturing, assembly, and support for global supply chains, making the incident potentially impactful to downstream manufacturers and partners.

Malaysian Architecture and Design Consultancy Listed on Genesis Ransomware Leak Site



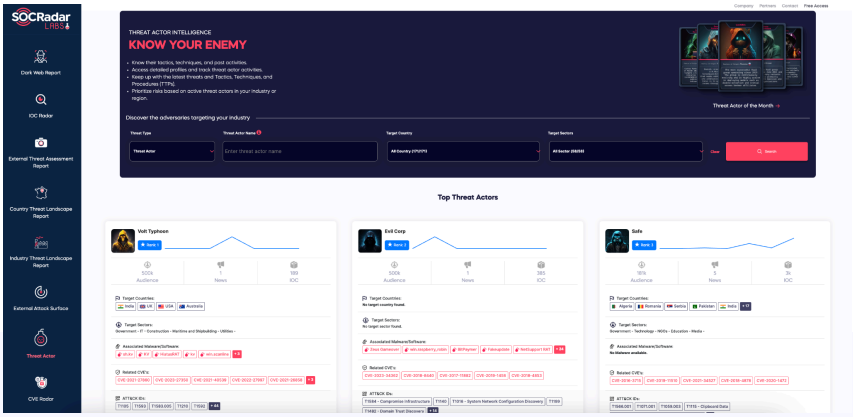
A Malaysian architecture and design consultancy specializing in public and private sector projects has been listed as a new alleged ransomware victim on the Genesis ransomware group leak site.

Malaysian Power Protection and UPS Provider Listed on SpaceBears Ransomware Leak Site



In the SpaceBears ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced involving a Malaysian company operating in the power protection and electrical equipment sector.

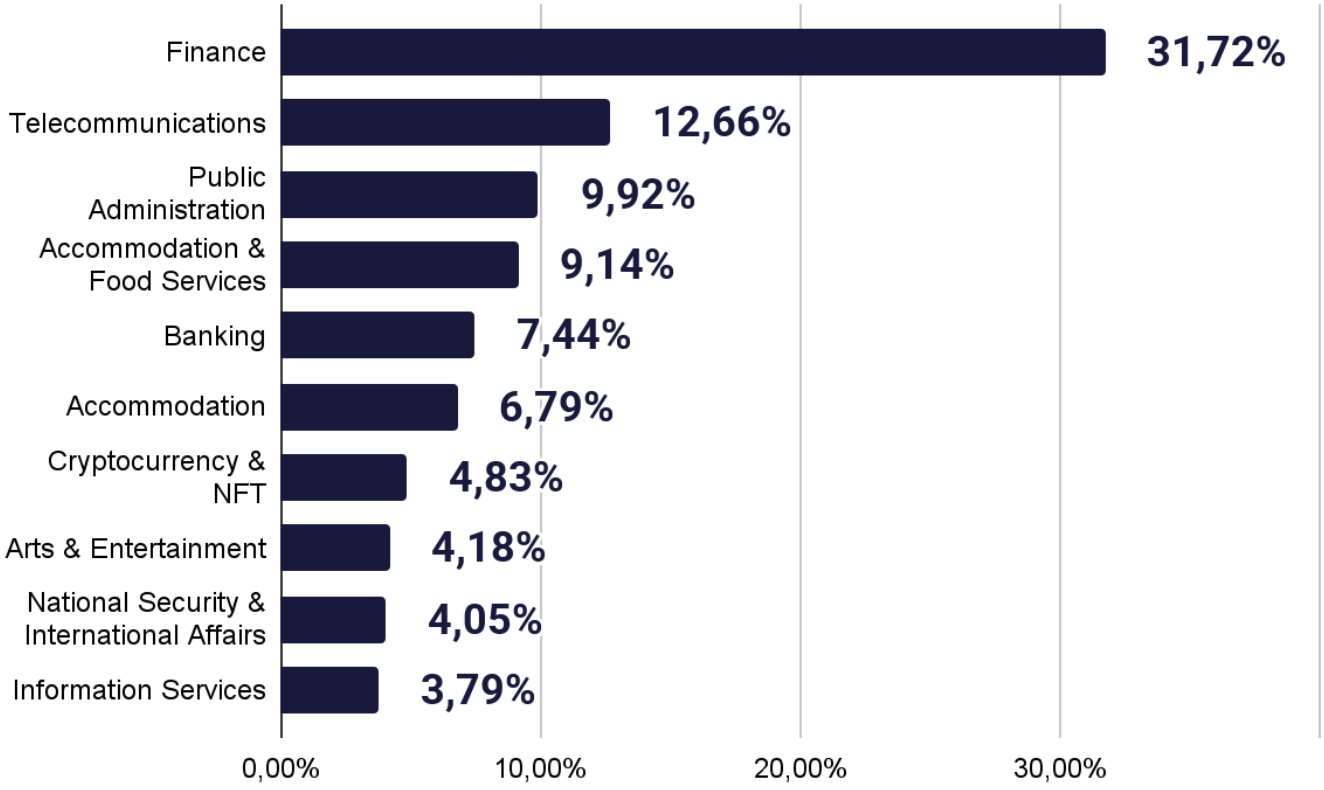
The organization provides UPS systems, industrial voltage regulators, batteries, and data center power solutions for business, education, and commercial environments. The leak allegedly includes employee and client personal data, as well as internal financial documents.



*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.*

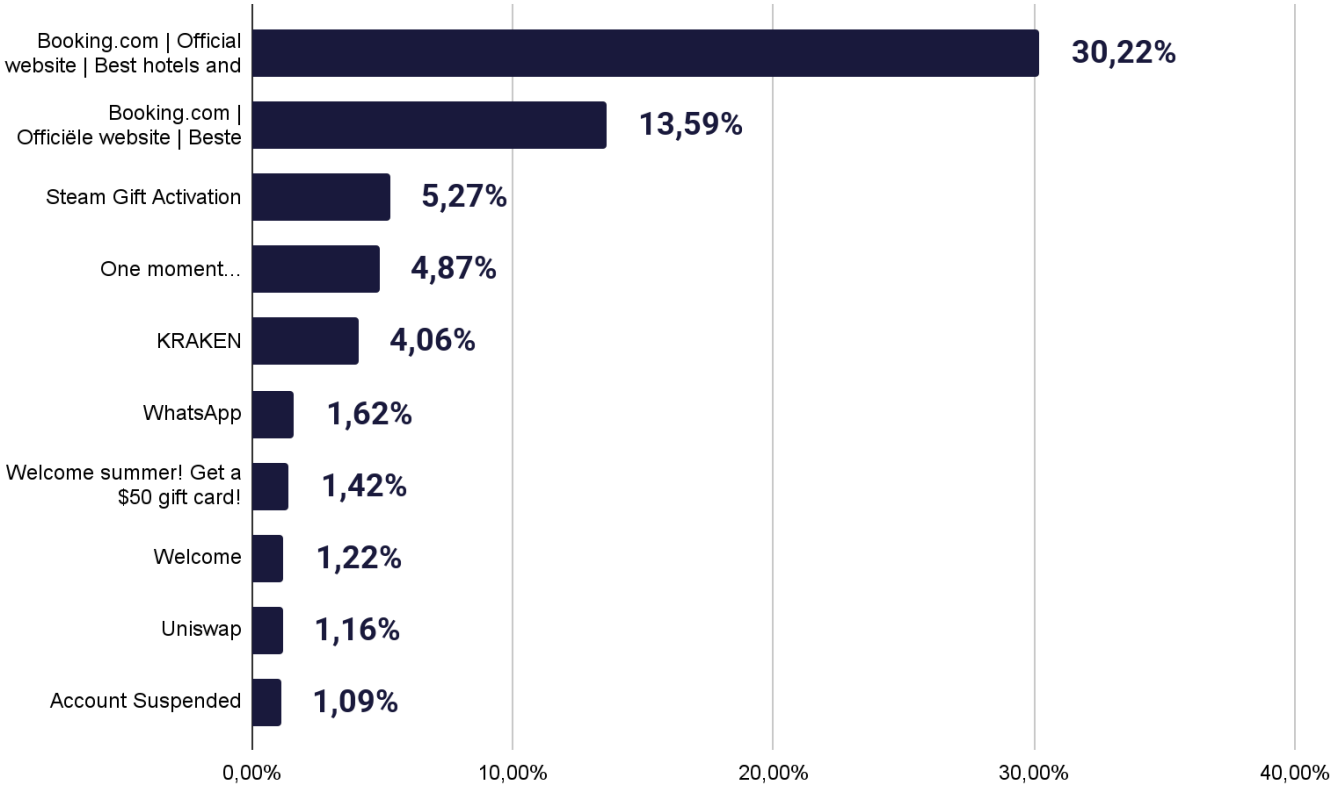
Phishing Threats Targeting Malaysia

Phishing Attacks - Distribution by Industry



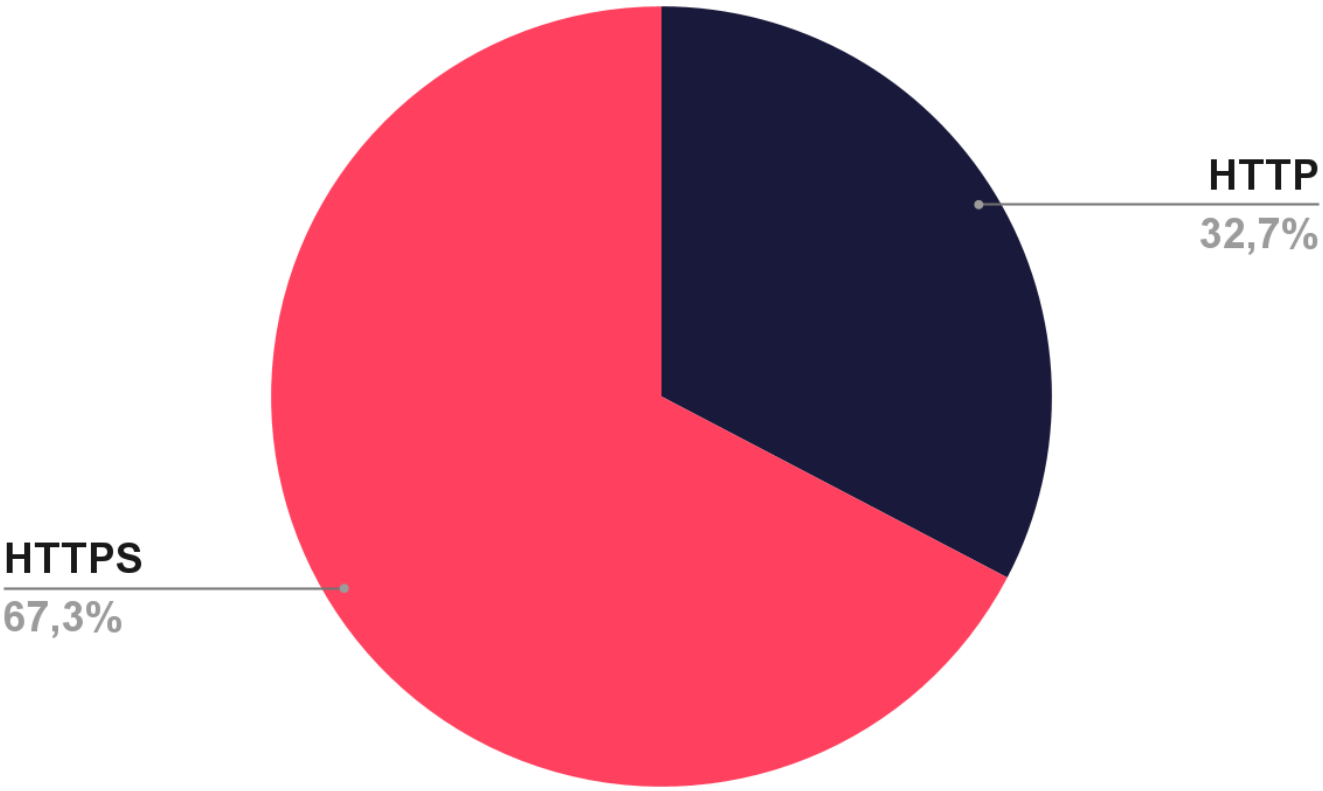
Phishing activity in Malaysia is strongly concentrated in the finance sector, which accounts for nearly one third of all observed cases. This reflects its direct link to monetary fraud and credential abuse. Telecommunications follows at a distance, likely due to its role in identity verification and SMS based scams. Public Administration also appears as a key target, which may support impersonation or social engineering campaigns. Accommodation and food related sectors show notable exposure, often linked to seasonal activity and high transaction volume. Overall, phishing targets sectors that combine high user interaction with financial or identity value.

Phishing Attacks - Distribution by Phishing Page Title



Phishing pages in Malaysia heavily rely on brand impersonation. Booking.com related titles alone account for more than 40 percent of observed cases, including multiple language variants. This indicates repeated reuse of proven templates rather than diverse lures. Gaming and crypto brands such as Steam, Kraken, and Uniswap appear but at much lower levels. Generic titles like “One moment” or “Account Suspended” suggest simple infrastructure that supports multiple campaigns. Overall, threat actors favor well known consumer platforms with high trust and large user bases, which increases click rates and credential capture success.

Phishing Attacks - Distribution by SSL/TLS Protocol



Most phishing threats targeting Malaysia use HTTPS, accounting for over two thirds of observed cases. This indicates widespread use of valid SSL certificates to appear trustworthy and bypass user suspicion. The continued presence of HTTP based phishing shows that basic and low effort campaigns still exist. However, the dominance of HTTPS reflects a shift toward more convincing phishing infrastructure. This trend reduces the effectiveness of user awareness based only on browser security indicators. It also increases the need for content inspection and behavior based detection rather than protocol level checks alone.

DDoS Attack Statistics

The threat landscape was pretty active for Malaysia.

- The **peak bandwidth** witnessed during a DDoS attack reached 353.7 Gbps, highlighting a significant capacity from the cyber threats.
- The **highest recorded throughput** during these incidents was 30.98 Mpps.
- Most DDoS attacks lasted **36.97 Minutes** on average.
- **120,849 Attacks** were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for Malaysia.

The numbers above show that Malaysia faces a serious DDoS risk. The attacks don't take too long, but the amount of attacks and their size are considerable threats to organizations.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks
DNS Amplification	39,964
STUN Amplification	33,905
TCP ACK	16,235
NTP Amplification	10,601
ISAKMP	7,090

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.

Who is SOCRadar?

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.

Trusted by
21.000+ companies
in 150+ countries

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.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

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.