SOCRadar
Your Eyes Beyond

Taiwan

Threat Landscape Report 2026

Executive Summary

Top Takeaways

- **Taiwan is a primary target, not collateral damage**
  80% of Dark Web threats and 65.60% of ransomware cases focus on Taiwan alone, showing that attackers build campaigns around Taiwan-specific victims rather than hitting the country as part of regional sweeps.

- **Government sectors lead both Dark Web and phishing activity**
  Public Administration tops the Dark Web ranking at 11.98%, while National Security & International Affairs (29.63%) and Public Administration (22.22%) together drive over half of all phishing attempts. This points to sustained espionage-style pressure on state institutions.

- **Manufacturing stands out among private-sector targets**
  At 9.50% of Dark Web activity, it reflects Taiwan's central role in semiconductor and electronics supply chains, making local producers a strategic target for data leaks and access sales.

- **The underground is a data marketplace**
  79.19% of threats involve databases, and 68.57% of activity is selling, confirming that stolen Taiwanese data is treated as a commercial product rather than shared for reputation alone.

- **Microsoft credentials are the top phishing prize**
  Microsoft-branded login pages account for nearly 67% of phishing titles, directly matching the heavy targeting of government and enterprise email accounts.

- **Local platforms are abused for trust**
  The Taiwanese short URL service yamShare appears in 13.10% of phishing cases, showing that attackers rely on familiar local brands to bypass filtering and suspicion.

- **Ransomware targeting is highly fragmented**
  Qilin leads at 18.7%, but 61.3% of attacks come from a long tail of smaller groups, meaning defenders cannot rely on blocking a few known actors and need behavior-based detection.

Technical Details

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

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

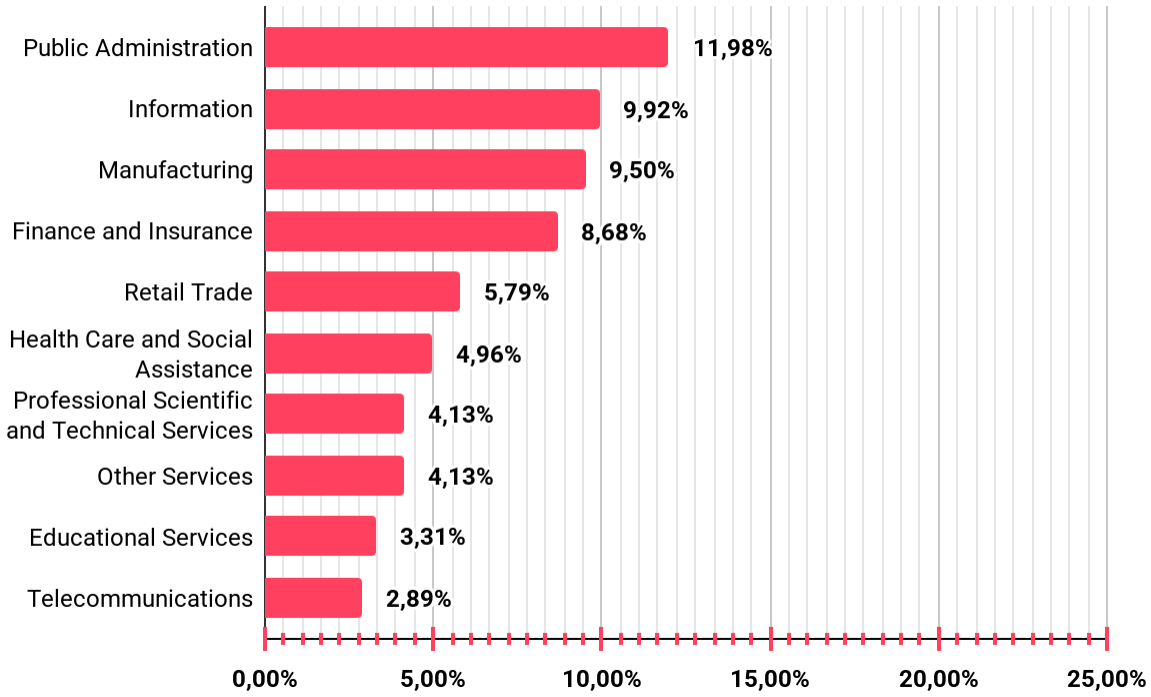
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups, and so on. These are areas where threat actors with various skill sets come together, discuss, share tools, and publish their alleged cyber attacks.

In the Ransomware Threats chapter, you will find detailed information about ransomware actors targeting Taiwan, 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 Taiwan

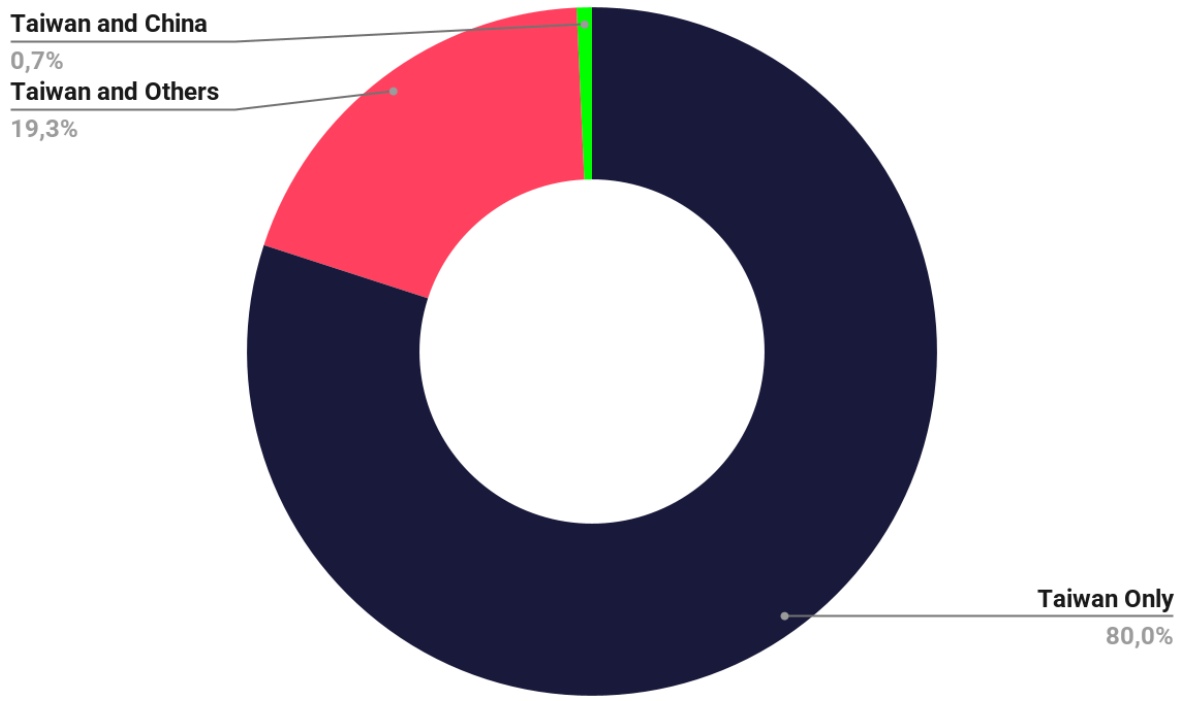
Distribution of Dark Web Threats by Industry



Public Administration leads the Dark Web threat distribution with 11.98%, reflecting the heavy targeting of government bodies in Taiwan. This is consistent with the island's geopolitical position, where state-linked and hacktivist actors often focus on public institutions to gather intelligence or cause disruption.

The Information sector (9.92%) and Manufacturing (9.50%) follow closely. Together with Finance and Insurance (8.68%), these top four industries account for roughly 40% of all Dark Web activity. The strong presence of Manufacturing is notable and likely tied to Taiwan's central role in global semiconductor and electronics supply chains, which makes local producers attractive targets for data leaks, access sales, and espionage-driven campaigns.

Distribution of Dark Web Threats by Primary Target Country



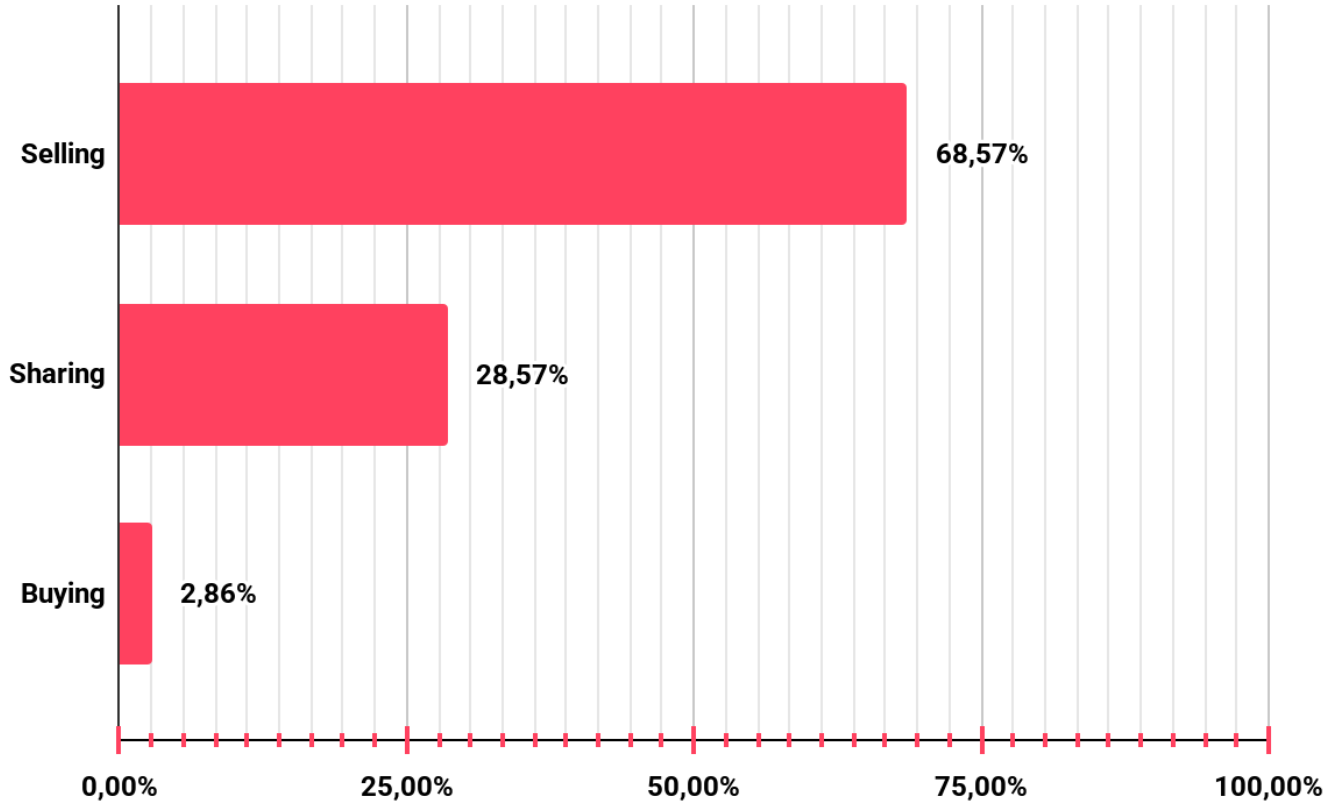
Taiwan is a primary target, not collateral damage

Among Dark Web threats involving Taiwan, 80% target it exclusively, which shows that threat actors are not hitting the country as collateral damage. Campaigns are built around Taiwan-specific victims, data, and access, pointing to deliberate and focused operations rather than broad regional sweeps.

The remaining 20% involves Taiwan alongside other countries. Within this mixed group, cases that pair Taiwan with China make up only 0.7% of the full dataset, a small but notable slice. These cross-strait cases often reflect shared-language phishing kits, actors working across Chinese-speaking regions, or campaigns tied to regional tensions.

Read together with the industry data, the picture becomes clearer. Public Administration and Manufacturing are heavily targeted, and most of that activity is Taiwan-only. This suggests that attackers treat Taiwan as a primary objective, not a secondary one, especially when government entities and semiconductor-linked manufacturers are involved.

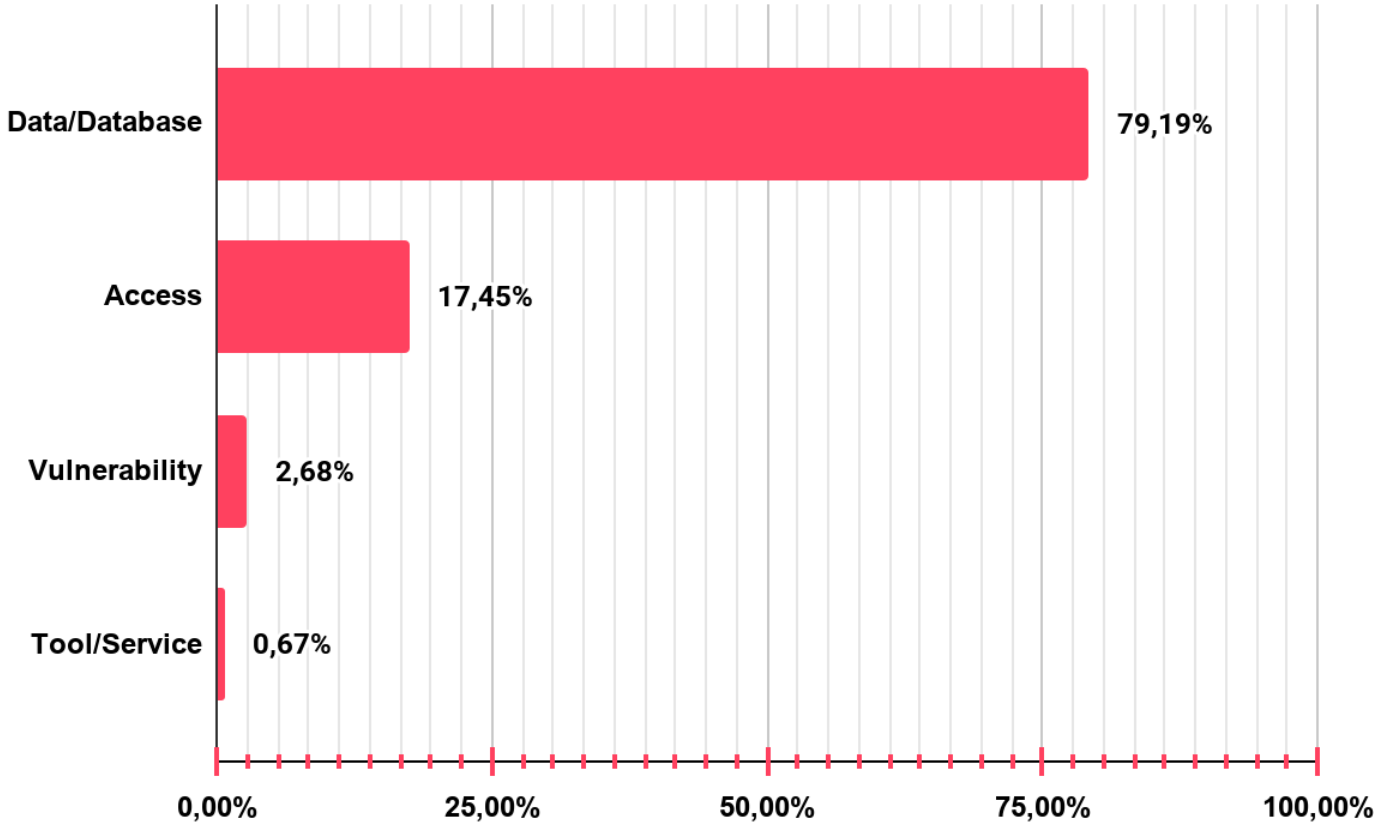
Distribution of Dark Web Threats by Threat Categories



Selling activity dominates the Dark Web landscape at 68.57%, showing that Taiwan-related data and access are treated as valuable commodities. Threat actors are not just leaking information for reputation; they are monetizing it. This pattern is common when victims include government bodies, manufacturers, and financial institutions, where stolen databases, corporate access, and credentials carry real market value.

Sharing follows at 28.57%. Free distribution often comes from hacktivist groups or actors looking to build credibility, and it also lowers the barrier for less skilled attackers who can reuse leaked data in follow-on attacks. This share is significant and suggests that ideologically driven activity plays a real role alongside financially motivated operations.

Distribution of Dark Web Threats by Threat Type



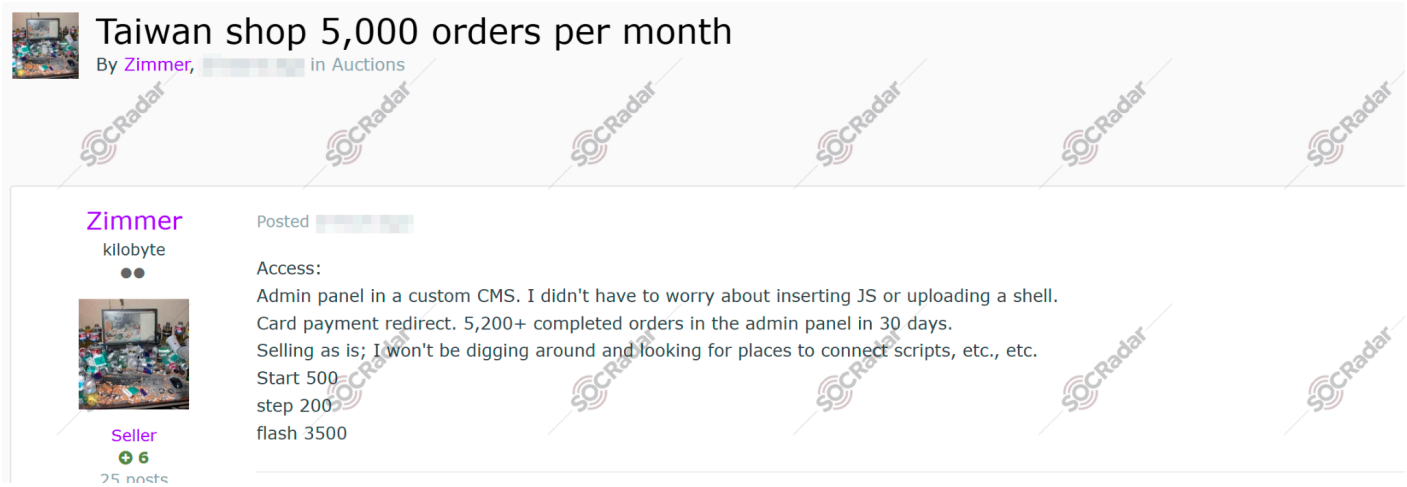
Data and database leaks make up 79.19% of all observed threats, confirming that stolen information is the core product on the Taiwan-focused Dark Web market. This aligns with the earlier finding that 68.57% of activity involves selling. Most of what is being sold are databases tied to government agencies, manufacturers, and financial firms, which explains why Public Administration and Information sectors lead the industry distribution.

Access-related listings follow at 17.45%. These include VPN credentials, RDP access, or admin panels, and they are a strong indicator of possible future intrusions. Buyers of access often move toward ransomware or espionage operations, so this category deserves close monitoring even if its share looks smaller.

Vulnerabilities (2.68%) and Tools or Services (0.67%) remain marginal. This suggests that the Taiwan-focused underground is more of a data marketplace than a hub for exploit development or offensive tooling, which is typically concentrated in larger, global forums.

Recent Dark Web Activities Targeting Entities in Taiwan

The Alleged Unauthorized Access Sale is Detected for a Taiwanese Shop



SOCRadar has detected a post on a Dark Web forum offering unauthorized access to an e-commerce shop operating in Taiwan. The access reportedly includes an admin panel on a custom CMS and a card payment redirect. The threat actor claims the shop processed over 5,200 completed orders in the past 30 days. The auction starts at $500, with increments of $200 and a flash price of $3,500.

Alleged Customer Database of a Taiwanese Consumer Chemicals Company Leaked on Dark Web Forum

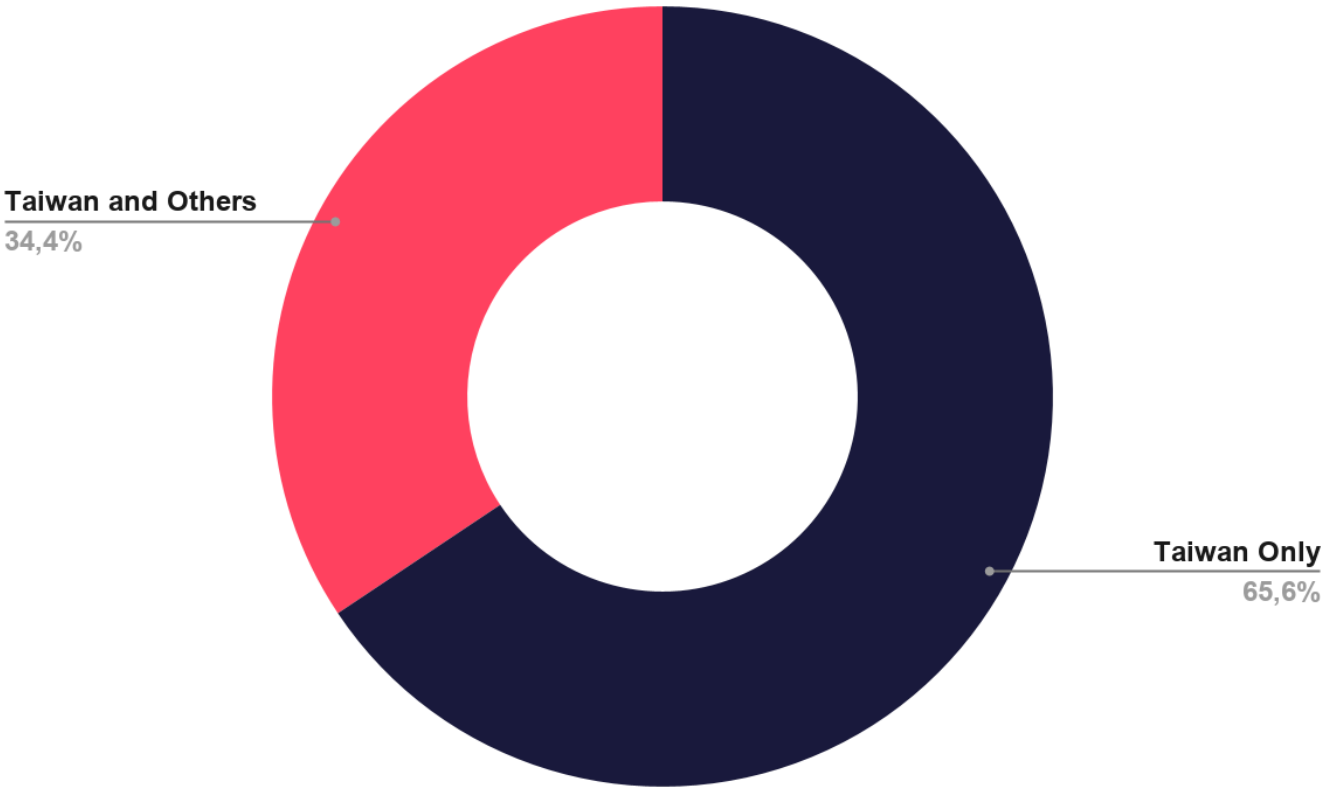
SOCRadar has detected a new alleged database leak on a Dark Web forum, targeting a consumer chemicals company operating in Taiwan. According to the post, the leak contains records of 12,299 customers. The compromised data reportedly includes IP addresses, names, gender, email addresses, countries, phone numbers, zip codes, counties and cities, areas, and physical addresses. The threat actor has made the database available for download.

Unauthorized Admin Access Sale Detected for a Taiwanese Manufacturing Company on Dark Web Forum

SOCRadar has detected a post on a Dark Web forum offering unauthorized admin access allegedly belonging to a manufacturing company operating in Taiwan. According to the post, the access includes Domain Admin privileges via AnyDesk. The auction starts at $1,250, with increments of $250 and a blitz price of $3,000.

Ransomware Threats Targeting Taiwan

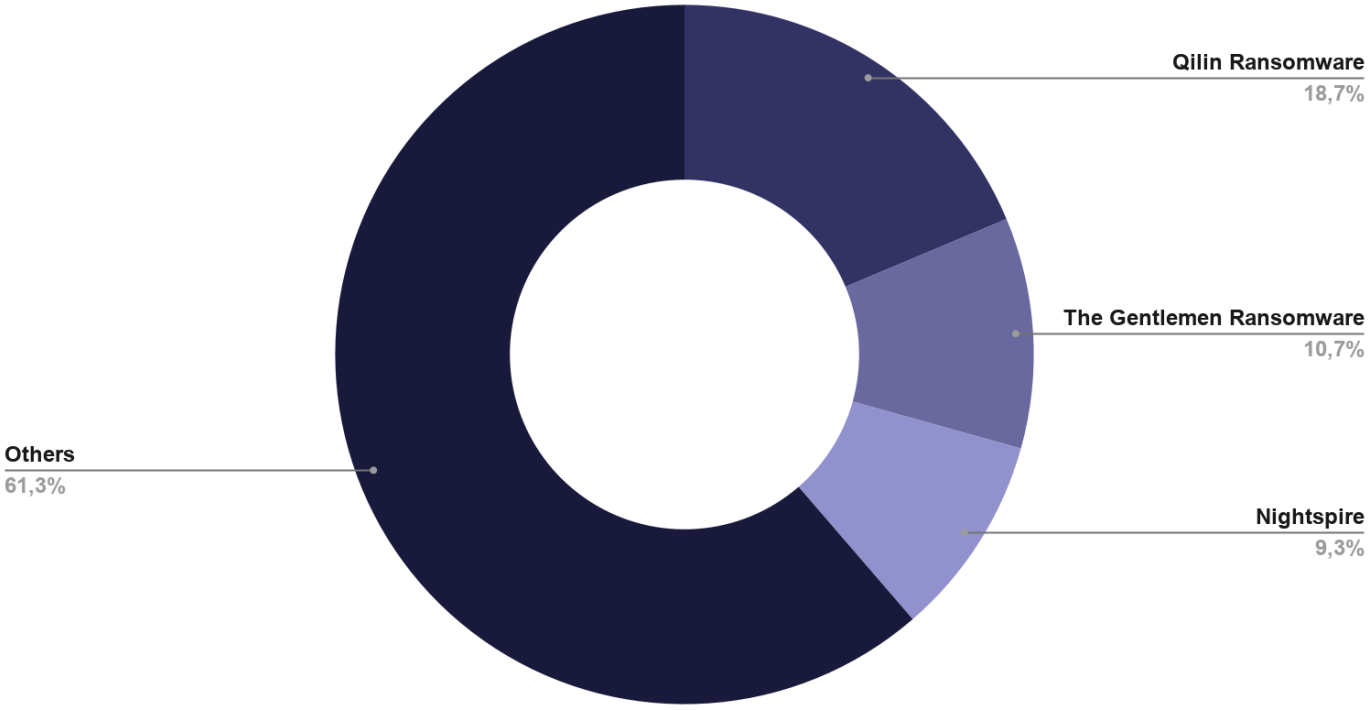
Distribution of Ransomware Threats by Primary Target Country



Ransomware groups focus on Taiwan alone in 65.60% of observed cases, while 34.40% of attacks hit Taiwan alongside other countries. Compared to the Dark Web threat distribution, where 80% of activity was Taiwan-only, ransomware shows a noticeably more international pattern.

Still, the fact that nearly two-thirds of ransomware incidents are Taiwan-only is significant. It suggests that a meaningful portion of ransomware activity is directed at Taiwanese organizations as local targets, not a part of an international campaign where the Taiwanese branch is also being affected. Manufacturing and other high-value sectors identified earlier are likely the main drivers of this focused targeting.

Top Ransomware Groups Targeting Taiwan



Qilin leads ransomware activity against Taiwan with 18.7% of observed cases, making it the single most active group in the dataset.

The Gentlemen (10.7%) and NightSpire (9.3%) follow. Both are newer groups that have gained visibility over the last year, and their appearance here suggests that Taiwan is on the radar of emerging operators, not only established ones.

The "Others" category at 61.3% is the most important signal. It shows that ransomware targeting Taiwan is highly fragmented, with no single dominant actor. Dozens of smaller groups and affiliates contribute to the overall volume. This fragmentation makes defense harder because each group uses different tools, negotiation styles, and leak site practices. Defenders cannot rely on blocking a handful of known actors. Accurate intelligence is more effective.

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.

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.

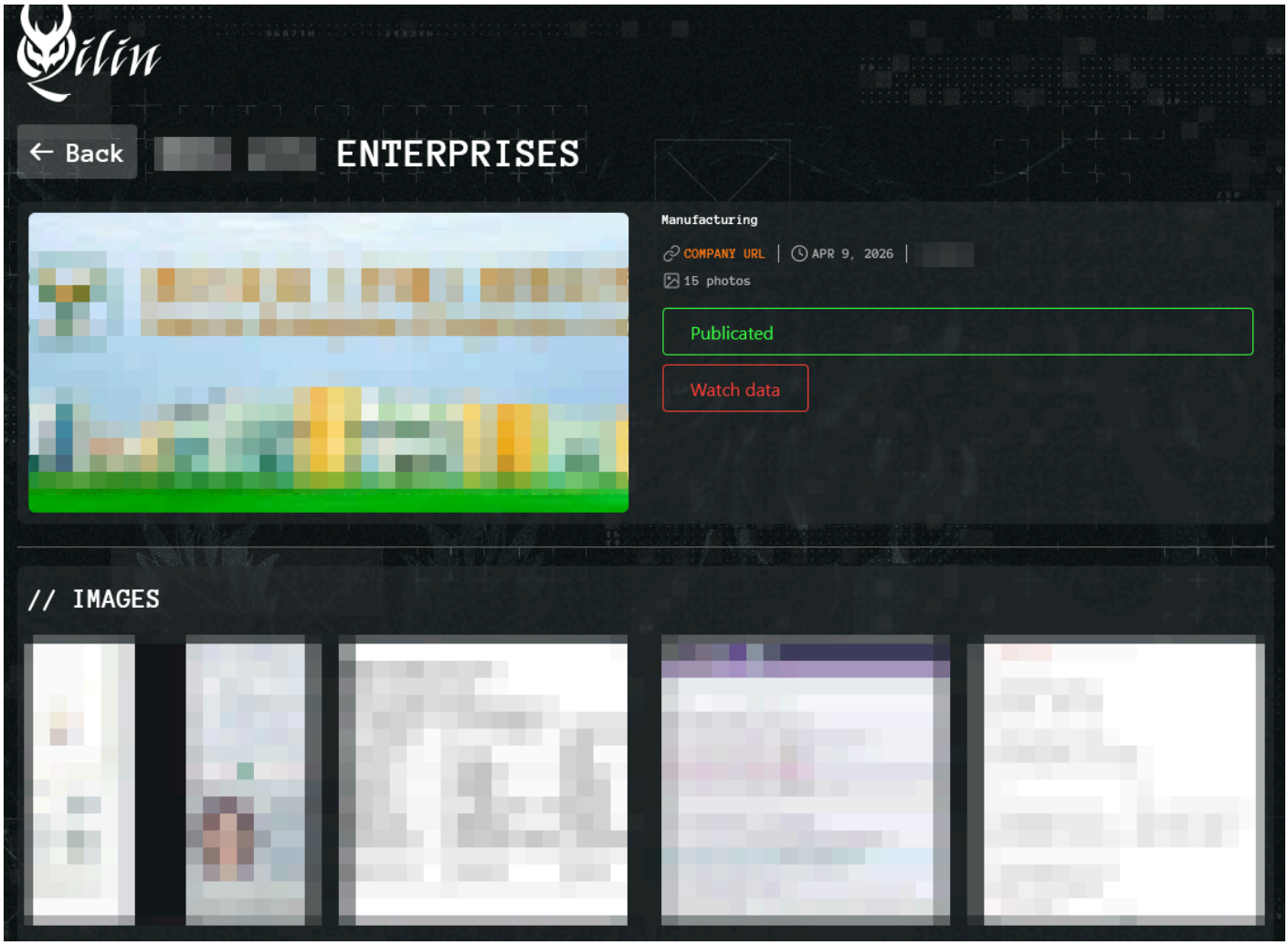
You can visit our blog post to read the rest of the threat actor profile.

Recent Ransomware Attacks Targeting Entities in Taiwan

Taiwanese Terminal Manufacturer Listed on The Gentleman Ransomware Leak Site

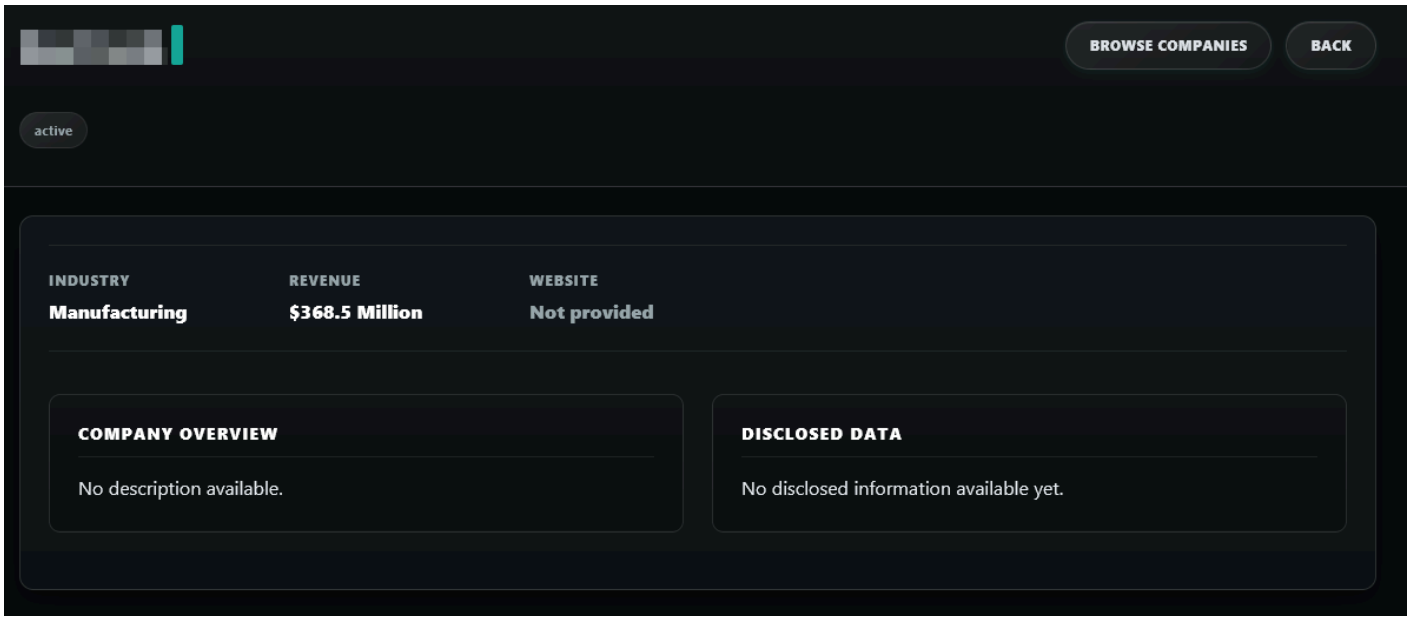
SOCRadar has detected a new post on The Gentleman ransomware leak site, targeting a company operating in Taiwan. The victim is engaged in the manufacture and sale of terminals used for electronic communication, automobile transportation, and electrical plugs. The company also offers ceramic ferrules, bushings, and modules.

Taiwanese Nonwoven Materials Manufacturer Listed on Qilin Ransomware Leak Site

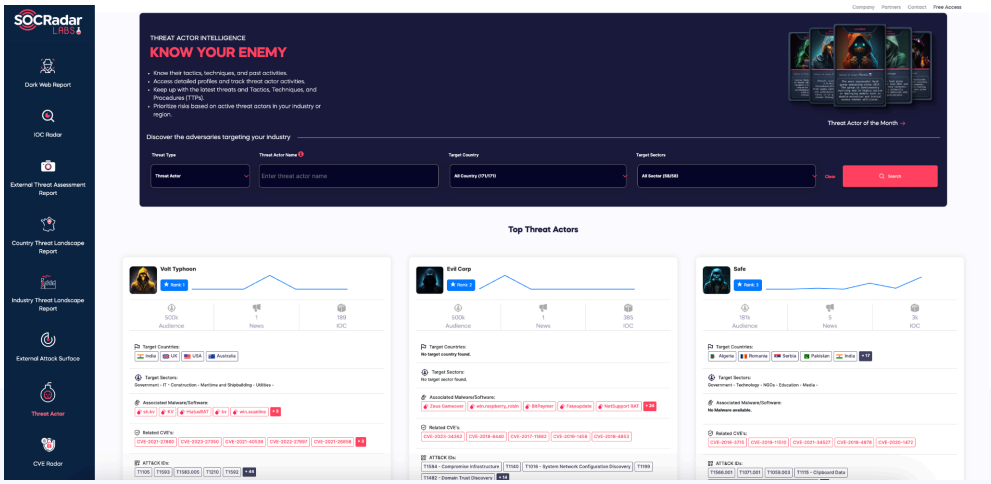


SOCRadar has detected a new post on the Qilin ransomware leak site, targeting a company operating in Taiwan. The victim is engaged in the production of nonwoven materials, including hygiene products, surgical gowns, medical bed sheets, and high-end dust-free wipes. The company also operates production facilities in China and India.

Taiwanese Acoustic and Audio Systems Manufacturer Listed on CoinbaseCartel Ransomware Leak Site



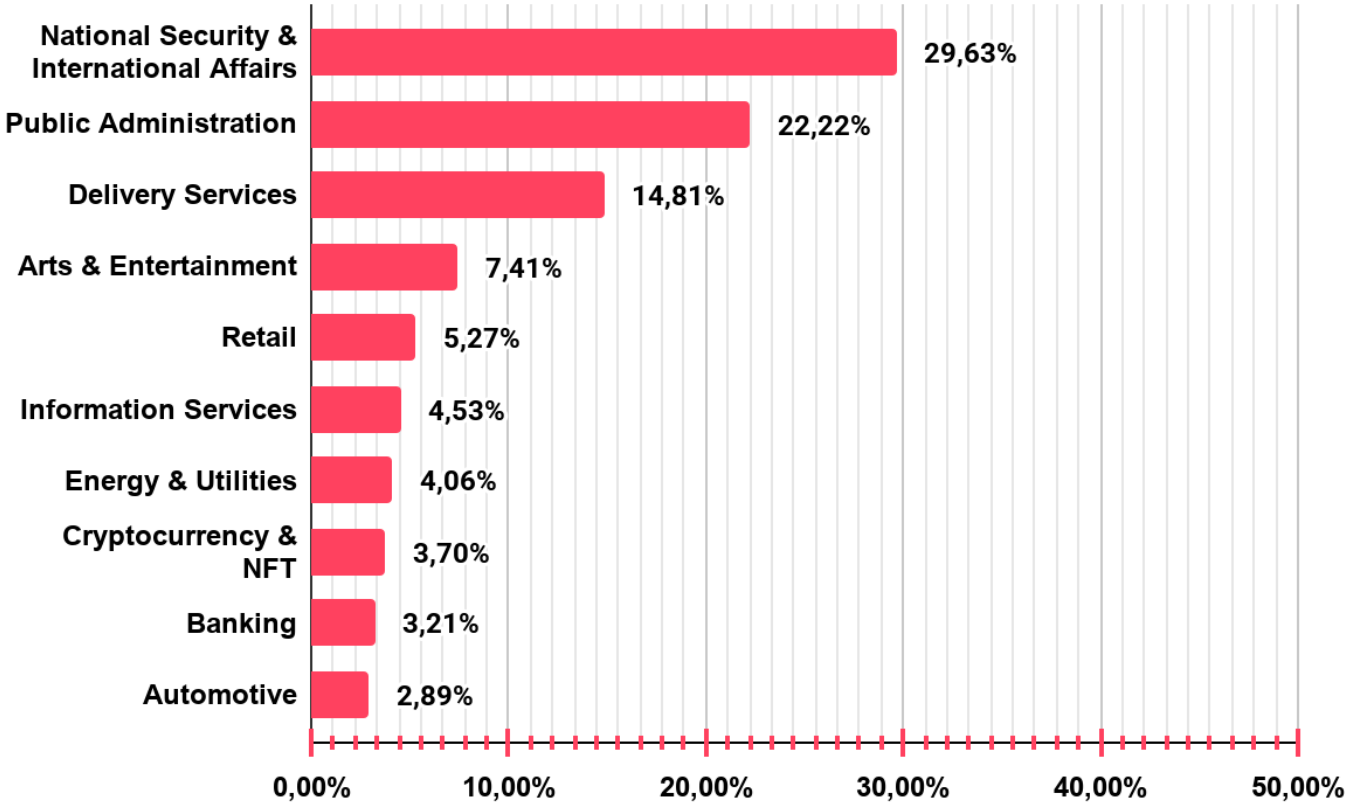
SOCRadar has detected a new post on the CoinbaseCartel ransomware leak site, targeting a company operating in Taiwan. The victim is engaged in the engineering, design, and manufacturing of acoustic modules, transducers, audio systems, and wearables. The company also provides original design manufacturing (ODM), joint design manufacturing (JDM), and electronics manufacturing services (EMS).



*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 Taiwan

Phishing Attacks - Distribution by Industry

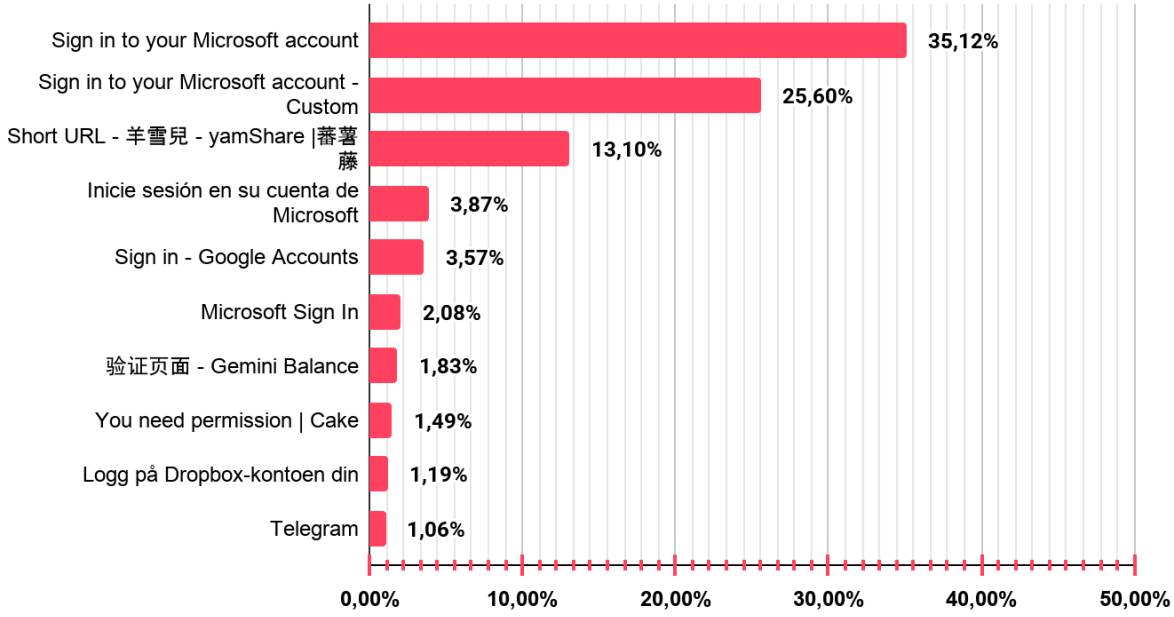


Phishing activity in Taiwan shows a very different pattern from the general Dark Web landscape. National Security and International Affairs leads with 29.63%, followed by Public Administration at 22.22%. Together, these two government-linked categories account for more than half of all phishing attempts. This points to targeted campaigns aimed at officials, diplomats, and public servants, which is typical of state-aligned or espionage-driven operations.

Delivery Services (14.81%) is the top private-sector target. Fake shipping and customs notifications are a common lure because they work on both individuals and corporate staff, and Taiwan's export-heavy economy makes these themes highly believable.

Arts and Entertainment (7.41%) and Retail (5.27%) reflect more opportunistic, consumer-focused phishing, often tied to ticketing and shopping scams. Financial targets such as Cryptocurrency and NFT (3.70%) and Banking (3.21%) appear lower in the ranking.

Phishing Attacks - Distribution by Phishing Page Title



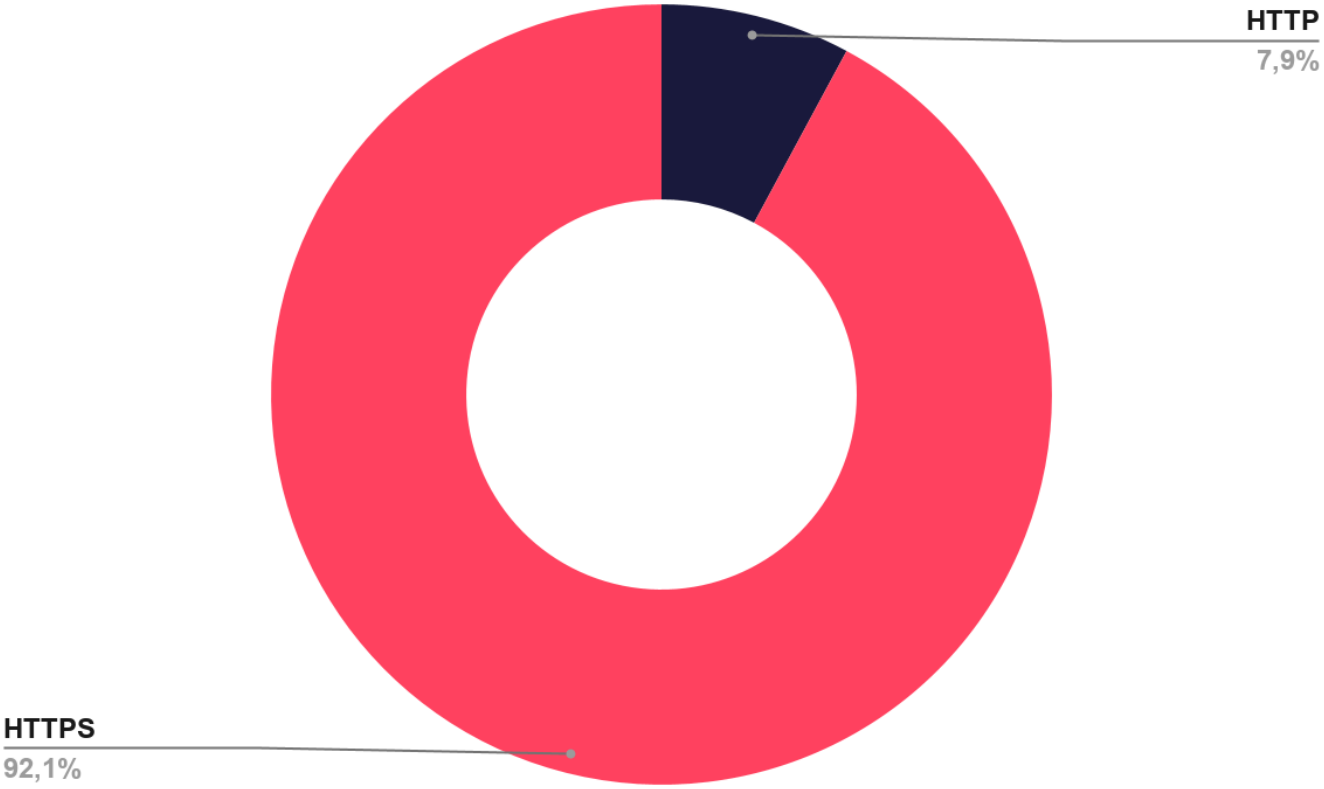
Local platforms are abused for trust

Microsoft-branded phishing pages dominate the landscape. The top two entries, "Sign in to your Microsoft account" (35.12%) and its custom version (25.60%), together make up over 60% of all phishing page titles. When the Spanish variant (3.87%) and "Microsoft Sign In" (2.08%) are added, Microsoft impersonation reaches nearly 67%. This confirms that Microsoft 365 and Outlook credentials are the most valuable target, which fits with the heavy focus on government and public administration sectors seen in the previous charts.

The Taiwanese short URL service "yamShare" appears in 13.10% of cases, showing that attackers use trusted local platforms to hide malicious links and bypass basic filtering.

Google Accounts (3.57%) and Dropbox (1.19%) follow at much lower levels. The presence of Spanish and Norwegian login pages suggests that some kits are recycled from global campaigns rather than built specifically for Taiwan, but the core targeting remains centered on corporate and government email access.

Phishing Attacks - Distribution by SSL/TLS Protocol



The vast majority of phishing pages targeting Taiwan, 92.10%, are served over HTTPS. Only 7.90% still rely on plain HTTP. This shows that attackers have fully adapted to modern web standards and are no longer cutting corners on encryption.

The reason is practical. Free certificates make HTTPS easy to deploy, and modern browsers now warn users strongly against HTTP sites. A phishing page without the padlock icon looks suspicious, while one with a valid certificate looks legitimate to most users. The padlock no longer proves safety; it only proves that the connection is encrypted.

Combined with the earlier finding that most phishing pages imitate Microsoft login screens, defenders need to rely on domain analysis, certificate transparency logs, and user training rather than simple protocol-based checks.

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.