foresiet

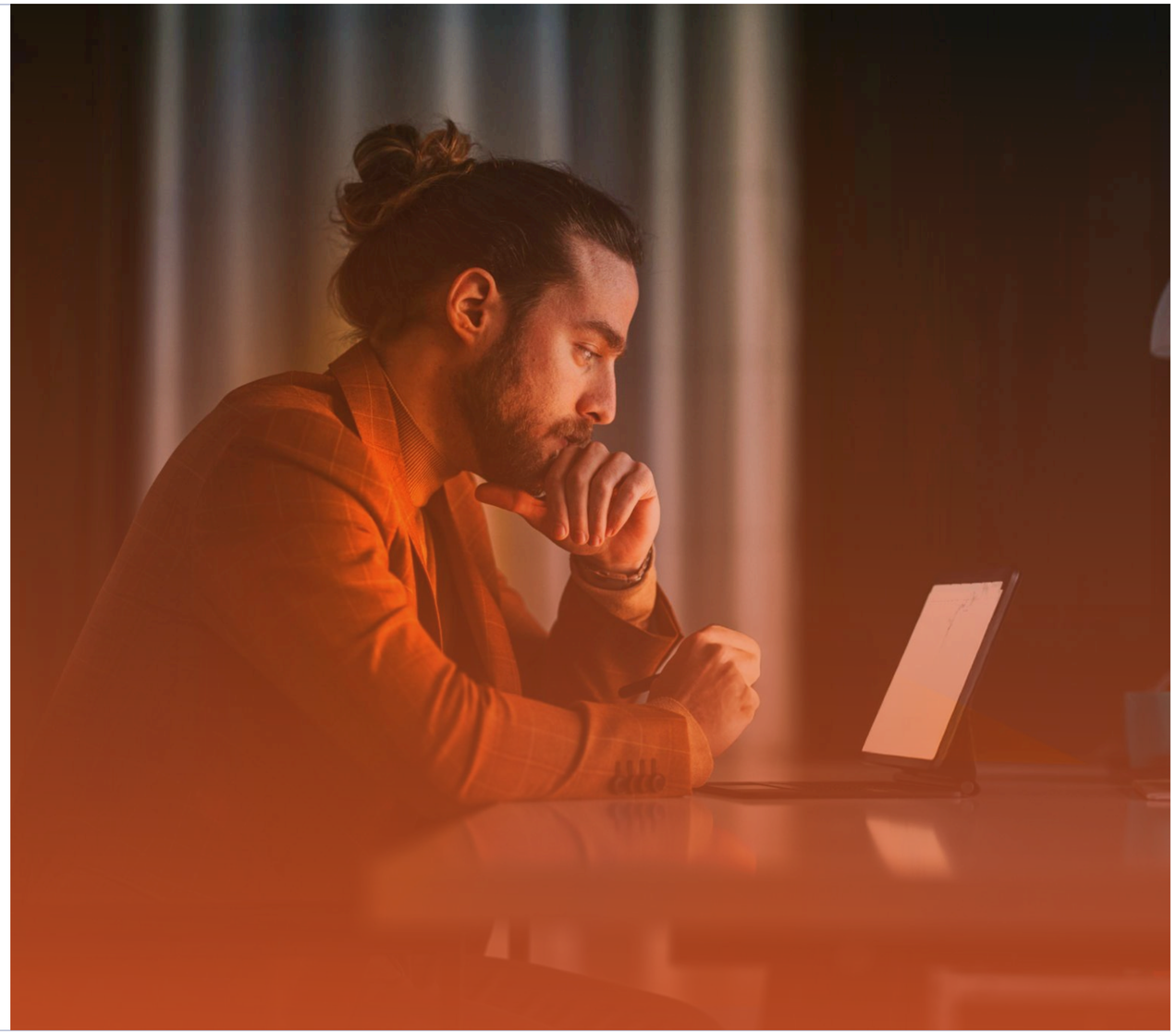
Vietnam Cybersecurity Report

Defending the Digital Frontier

January- April 2025

Table of Contents

01
Introduction



Vietnam’s accelerating digital transformation has brought significant economic and societal benefits — but it has also drastically expanded the nation’s cyber threat surface. As Vietnam pushes toward becoming a leading digital economy in Southeast Asia, it is witnessing a sharp rise in targeted cyber activities.

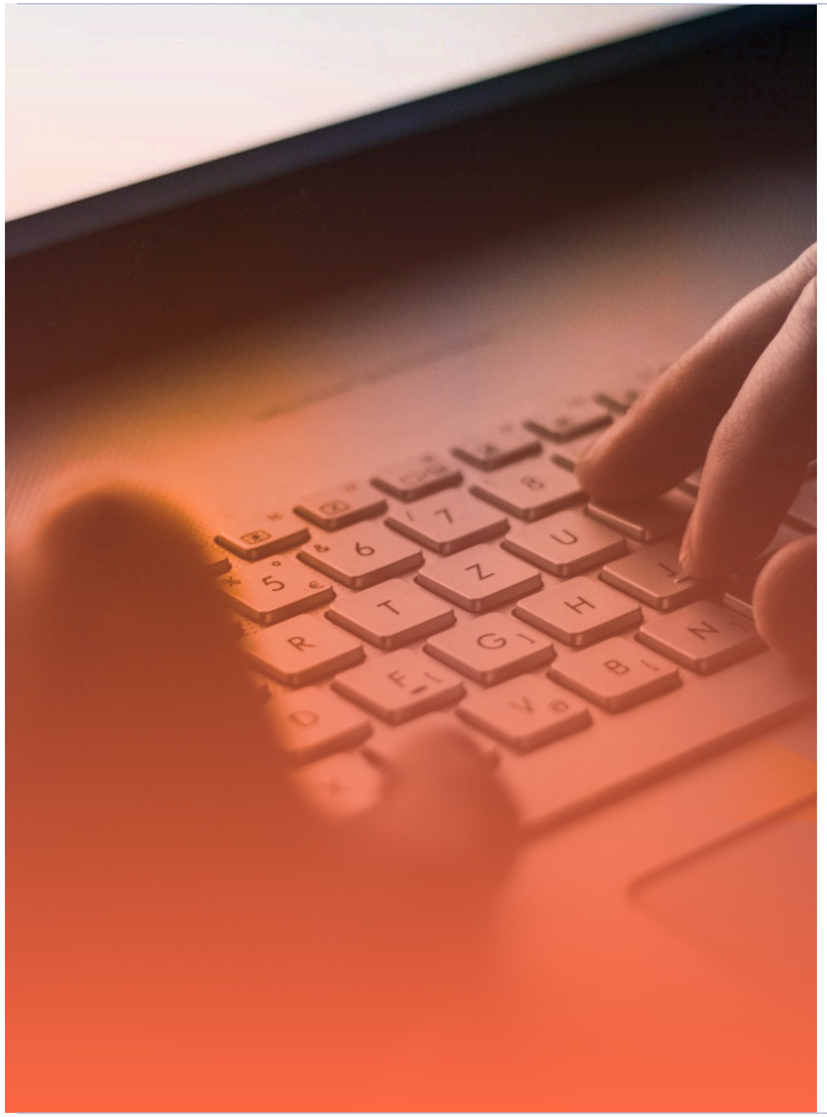
Between January and April 2025, Vietnam ranked among the most targeted countries in the Asia-Pacific region, according to regional cybersecurity intelligence. The country's growing reliance on cloud infrastructure, e-government platforms, and domestic tech manufacturing has attracted the attention of cybercriminal groups and state-sponsored threat actors alike.

Key sectors such as public infrastructure, digital banking, e-commerce, and the media have been subjected to sophisticated cyberattacks, including coordinated disinformation campaigns, data breaches, and distributed denial-of-service (DDoS) operations. Meanwhile, Vietnam’s strategic role in the regional supply chain — especially in semiconductors, electronics, and AI technologies — has made it a critical target for cyberespionage.

Compounding these threats is the challenge of fragmented security policies across provinces, varying levels of institutional preparedness, and limited cyber literacy among small and medium-sized enterprises (SMEs).

As Vietnam prepares to scale its digital economy under the “National Digital Transformation Program by 2025,” improving its cyber resilience and national cyber threat intelligence sharing has never been more vital. Proactive investments in security operations, public-private collaboration, and advanced threat detection are essential to safeguarding Vietnam’s digital future.

02
Executive Summary



From January to April 2025, Vietnam faced a sharp escalation in cyber incidents that highlighted its growing vulnerability amid rapid digital expansion. Threat actors targeted critical sectors including government, education, media, and ICT services — using a combination of DDoS attacks, ransomware, and network intrusions. These incidents exposed systemic gaps in cyber resilience and raised alarms across the region.

Major Incidents

January–March 2025: The hacktivist collective AnonymousVNLBN, believed to be loosely affiliated with regional cyber activists, launched a coordinated wave of distributed denial-of-service (DDoS) attacks. Government platforms and education portals, including provincial e-learning systems and public service websites, were taken offline for hours to days. These attacks caused significant service disruptions and forced some agencies to revert to offline operations.

April 12, 2025: One of Vietnam's leading ICT services firms — a key provider of network and cloud infrastructure to state-owned enterprises and multinational corporations — was hit with a double-extortion ransomware attack. The attackers not only encrypted critical systems but also exfiltrated sensitive customer and government data. The breach led to a complete infrastructure shutdown lasting more than 72 hours and prompted urgent incident response at a national level.

Late April 2025: Multiple state-backed media outlets were breached in a coordinated operation suspected to be the work of foreign advanced persistent threat (APT) actors. Attackers gained editorial access, defaced web content, and exfiltrated internal communications and unreleased political narratives. Some of the compromised documents later surfaced in disinformation campaigns on Telegram and X (formerly Twitter), aiming to destabilize trust in official institutions.

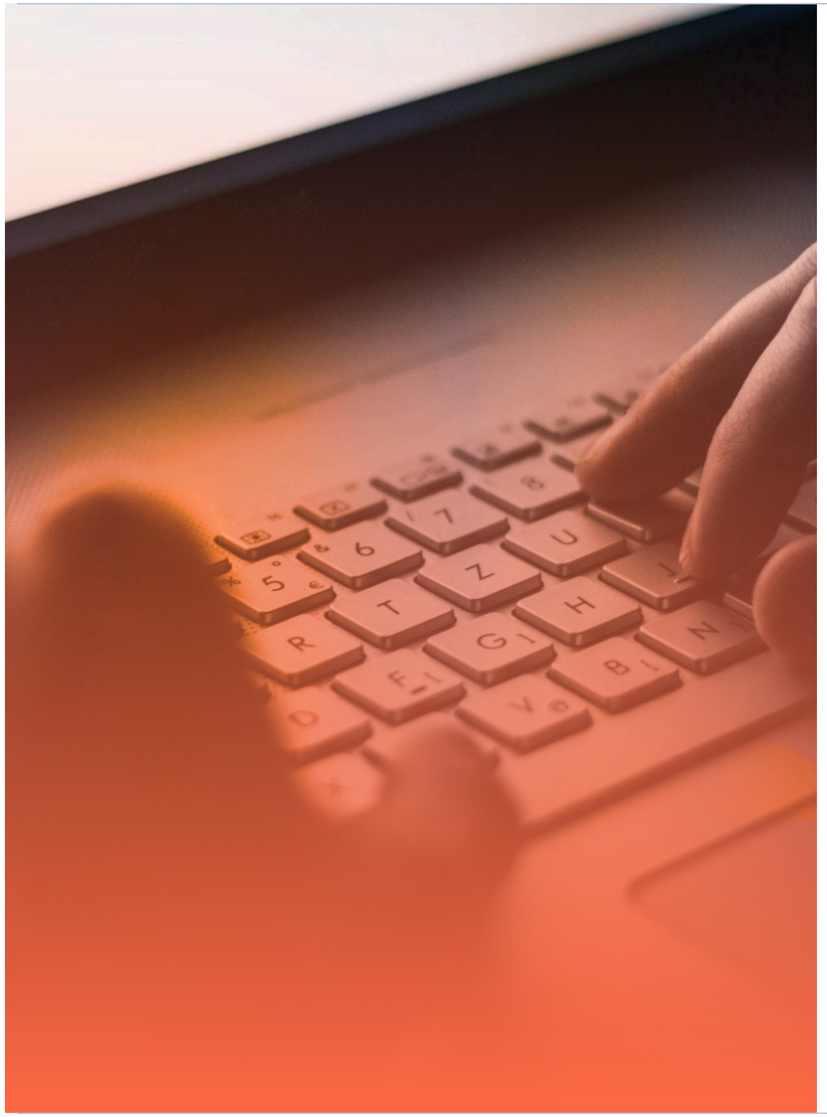
Sectoral Impact

Government:
The disruption of public portals and data theft from state-linked entities reflected a rising trend in politically motivated attacks.

Education:
DDoS attacks crippled several online learning platforms, especially during examination periods.

Media:
Breaches impacted press integrity and exposed the media to foreign influence operations.

ICT/Private Sector:
The ransomware attack signaled the rising threat of financially motivated cybercriminals targeting Vietnam’s critical infrastructure providers.



Overall Assessment

These incidents indicate a maturing threat landscape in Vietnam, with both ideological and profit-driven actors actively targeting national assets. The attacks were marked by increasing sophistication, including the use of proxy servers, AI-generated phishing content, and custom malware. While authorities responded swiftly in some cases, the need for enhanced cyber threat intelligence, multi-stakeholder coordination, and improved incident response mechanisms remains evident.

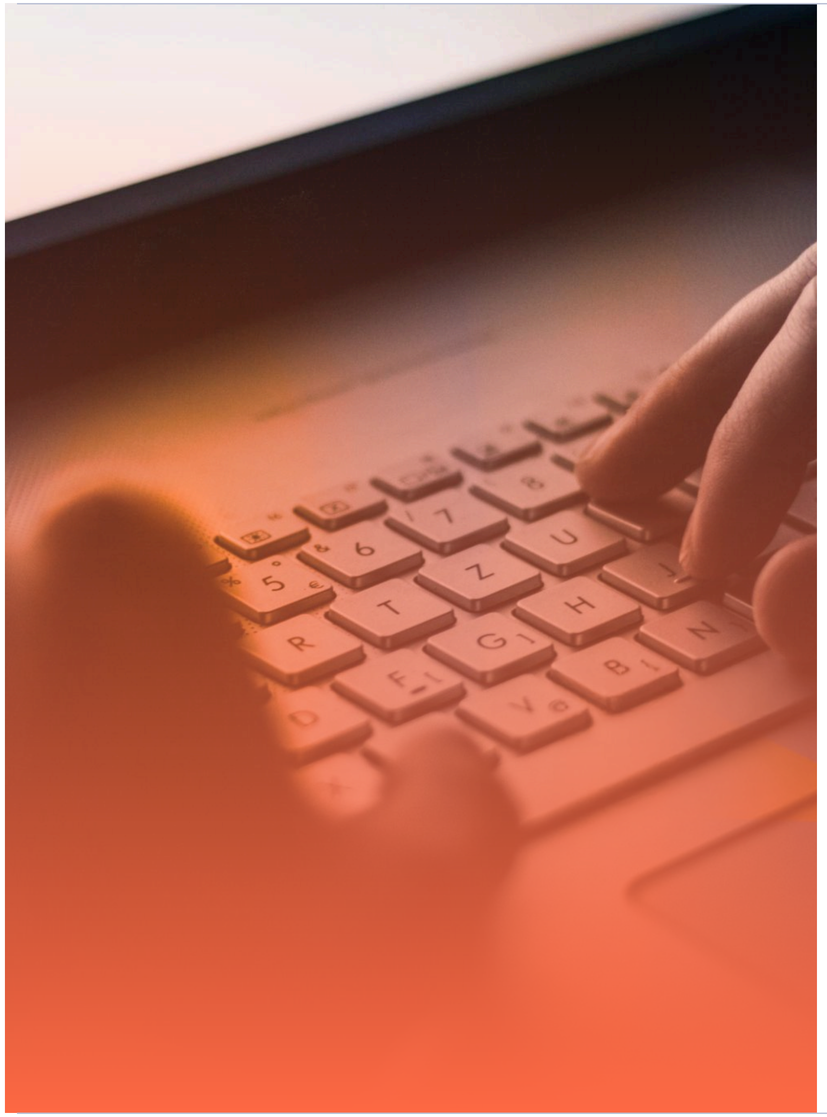
Most Affected Sectors

The cyberattacks during the January–April 2025 period disproportionately impacted several high-value sectors critical to Vietnam's digital infrastructure and public trust:

ICT and Technology Service Providers
As the backbone of Vietnam's digital transformation, ICT firms emerged as primary targets. The April ransomware attack on a major provider crippled cloud, hosting, and managed service environments across multiple industries. The compromise of supply-chain providers raised concerns about national digital dependency on single service points.

Media and Communications Organizations:
State-affiliated media outlets were breached in late April, exposing editorial systems and triggering coordinated disinformation campaigns. These compromises not only disrupted media operations but also posed broader national security concerns as attackers manipulated public perception and spread politically charged narratives.

Government and Educational Institutions:
Public service platforms — especially in provincial governments — faced repeated DDoS attacks, affecting services like e-Citizen, taxation, education portals, and district-level administration systems. Schools and universities also reported disruptions to exam portals and internal communications, largely driven by smishing and botnet-driven DDoS attacks.



Economic & Operational Impact

The surge in cyberattacks during 2025 has translated into significant operational and economic consequences:

High Downtime Costs:

Organizations hit by ransomware and DDoS attacks were forced to isolate systems and activate disaster recovery protocols. These emergency responses led to prolonged service outages, increased operational expenses, and reputational damage. Some firms estimated recovery costs in the range of tens of billions of Vietnamese dong (VND).

Public Mistrust in Media:

The compromise of state-linked media sites caused widespread concern over the authenticity of news content. With forged editorials and deepfake videos circulating post-breach, public confidence in official narratives declined, especially among younger internet-savvy demographics.

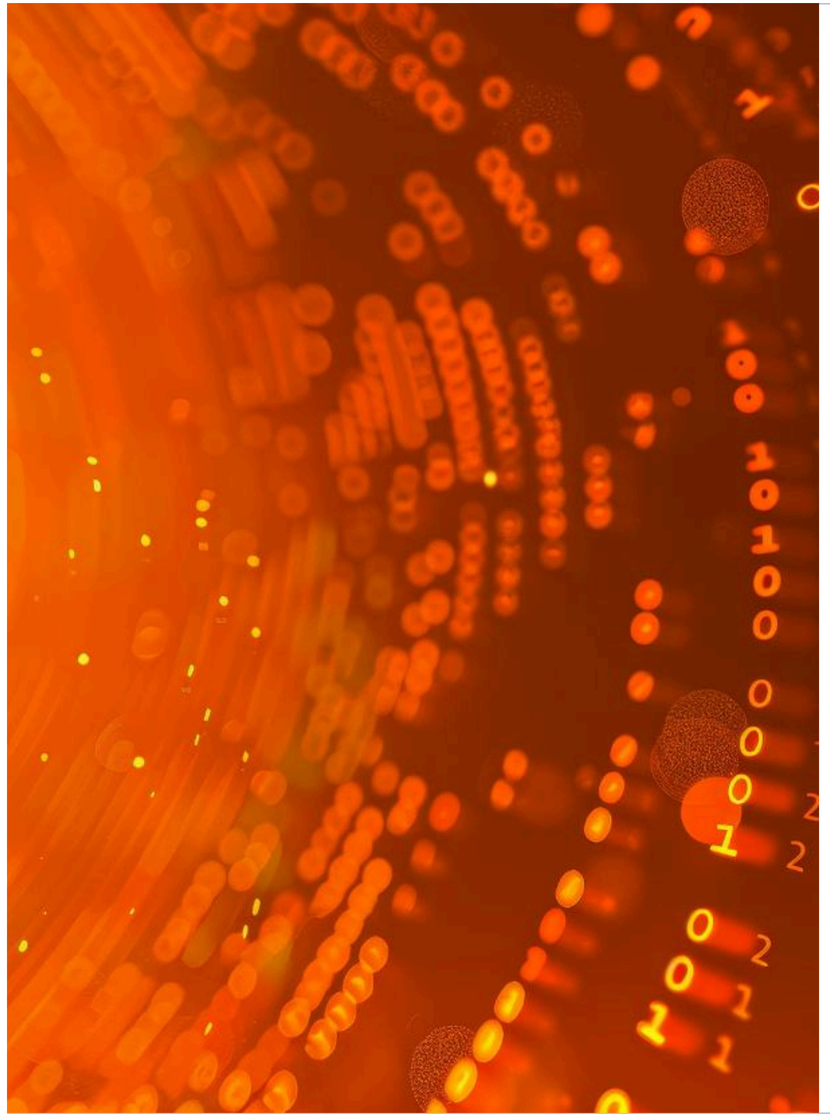
Administrative Disruption:

The DDoS campaigns disrupted access to essential services such as tax filing, academic exam results, and health records. This forced some government departments to revert to manual processes, delaying service delivery and undermining trust in Vietnam's digital governance model.

Vietnam's Cyber Crisis: January-April 2025

- **January-March 2025** — DDoS attacks by AnonymousVNLBN disrupt government and education platforms
- **April 12, 2025** — Ransomware attack on ICT services firm leads to infrastructure shutdown
- **Late April 2025** — Media outlets breached, disinformation campaigns launched

03
Emerging Threat Trends



Between January and April 2025, Vietnam experienced an evolving range of cyber threats characterized by stealth, deception, and increased technical sophistication. Cybercriminals and advanced persistent threat (APT) actors leveraged emerging technologies and user behavior trends to compromise systems, exfiltrate data, and disrupt operations. The following are the key emerging threats observed during this period:

SteelFox Trojan Campaign

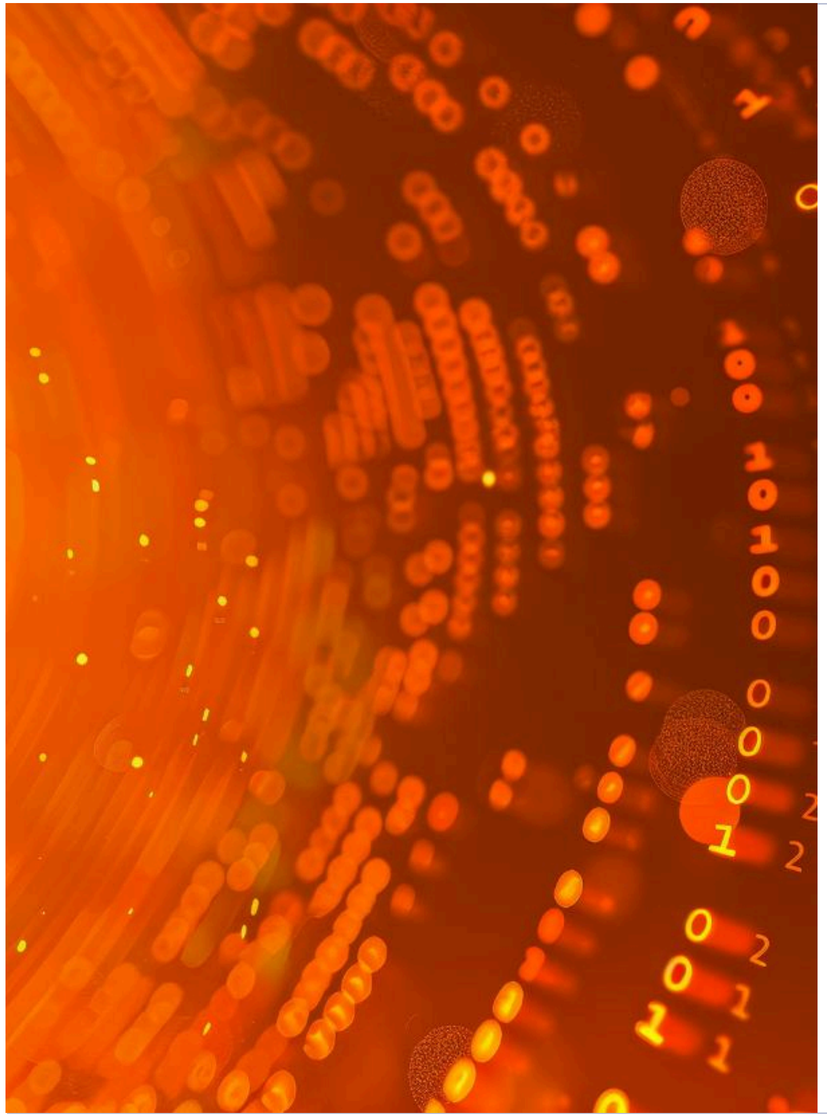
A widespread malware campaign dubbed SteelFox emerged in early 2025, targeting Vietnamese consumers through cracked software and pirated Windows activators. This multi-functional trojan combines information stealing and crypto-mining capabilities. It hijacks system resources for Monero mining while silently exfiltrating browser-stored credentials, Discord tokens, and keystrokes. Cybersecurity firms in Vietnam confirmed hundreds of infections across Hanoi and Ho Chi Minh City, mostly among students and small office/home office (SOHO) users. The campaign exploited Vietnam's high rate of software piracy and limited endpoint protection in personal environments.

SpyLoan Android Malware

A surge in deceptive mobile lending apps — part of the SpyLoan malware family — was observed across Vietnamese app ecosystems and third-party APK sites. Masquerading as urgent loan services, these apps harvested users' contact lists, SMS logs, GPS data, and in some cases, recorded audio. The malware also tracked behavioral patterns and was used to blackmail users who defaulted on fake loan terms. Reports suggest links to regional crimeware groups operating across Southeast Asia, with Vietnam being a major test market due to high smartphone penetration and fintech adoption.

APT41's DeepData Espionage Operation

Cyber threat intelligence indicated signs of ongoing activity from APT41, a China-linked threat actor known for dual-purpose cybercrime and espionage. Between March and April 2025, Vietnamese telecom providers were probed using custom reconnaissance tools, in what appears to be the early phase of DeepData, an operation aimed at mapping regional telecom infrastructure. Although no public disclosures were made, internal scans and beacon traffic patterns were detected by private sector security teams working with CERT Vietnam. This suggests potential pre-positioning for future data exfiltration or surveillance.



IoT Botnets

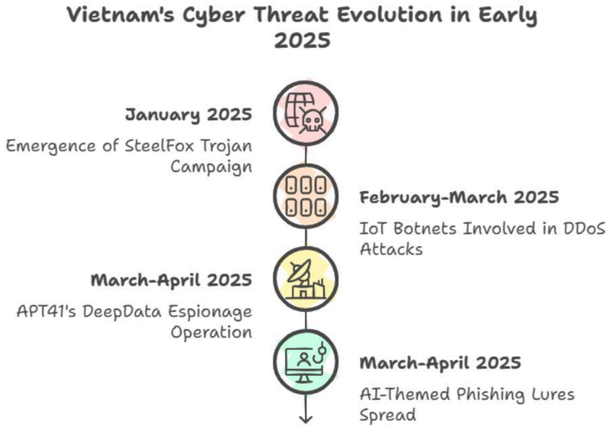
Vietnam continued to be a hotbed for IoT botnet recruitment, with compromised routers, CCTV systems, and smart TVs used in botnet-driven DDoS attacks. Devices from local OEM brands with default or hardcoded credentials were especially vulnerable. Security vendors reported the return of Mirai and Gafgyt variants, actively scanning IP blocks in Vietnam. These botnets were involved in flooding educational and government portals with junk traffic in February and March 2025, likely connected to the AnonymousVNLBN hacktivist campaigns.

AI-Themed Phishing Lures

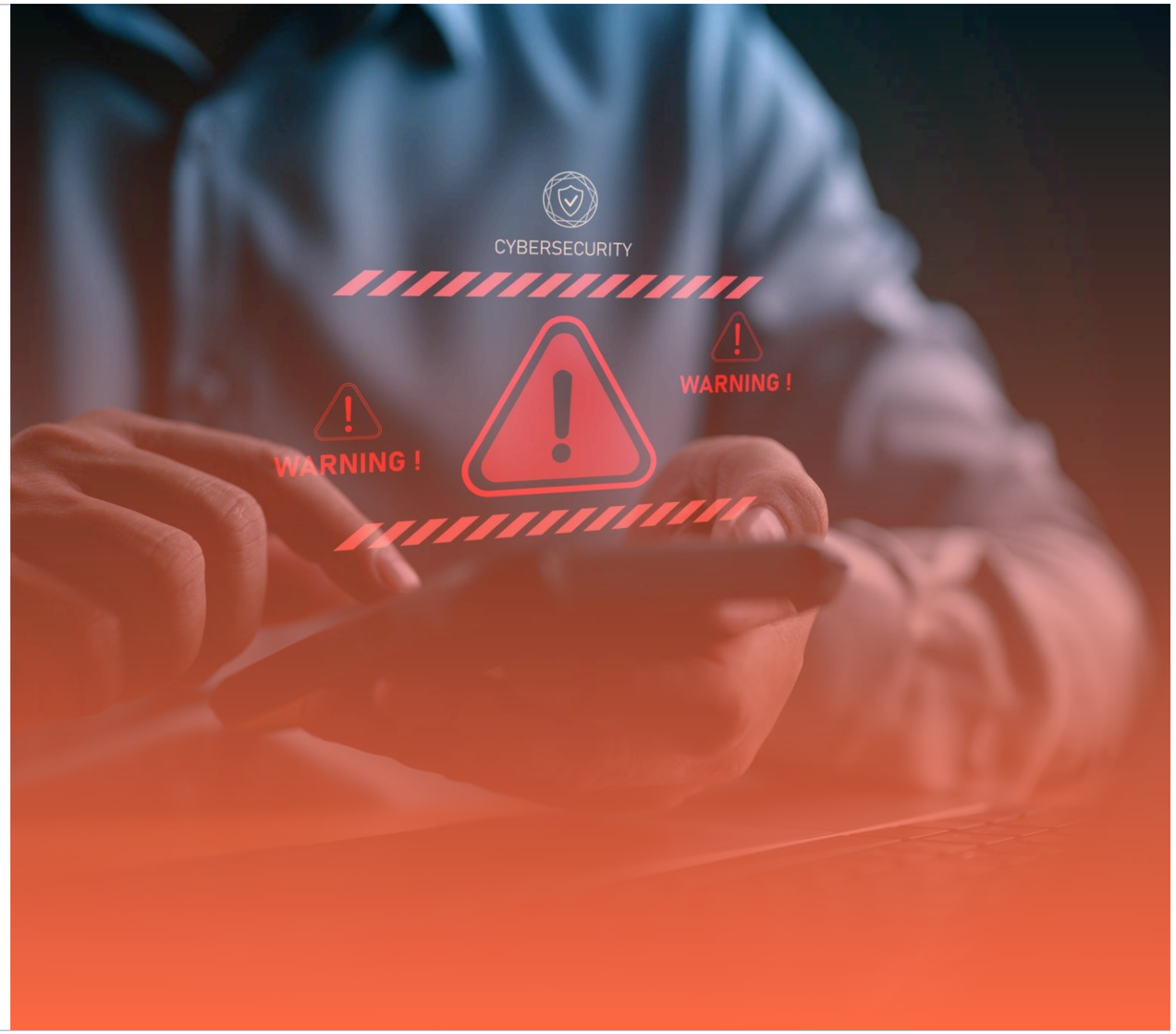
Capitalizing on the regional hype around generative AI, threat actors began spreading phishing links disguised as AI-powered productivity tools, Vietnamese-language chatbots, and resume boosters. Once downloaded, these tools delivered info-stealing malware (such as RedLine and Vidar) or deployed remote access trojans (RATs) via malicious PowerShell payloads. Young professionals and freelancers were especially targeted through Facebook Messenger and LinkedIn, with attackers tailoring lures in Vietnamese and English.

Cybersecurity analysts in Da Nang and Hue flagged over 20 clone domains impersonating popular AI tools.

These trends demonstrate that cyber threats in Vietnam are not only increasing in volume but also diversifying in approach — leveraging local socio-economic conditions, digital behavior, and technological trends to maximize impact. Continued vigilance, threat intelligence sharing, and public cyber hygiene awareness are crucial in responding to this expanding threat landscape.



04
Attack Techniques Overview



Vietnam's cyber threat landscape in early 2025 has been marked by an uptick in both opportunistic and targeted attacks using a variety of sophisticated methods. Threat actors employed multi-layered tactics blending traditional vectors with emerging tools such as fake AI applications and custom ransomware strains to compromise networks, disrupt services, and steal sensitive information.

Ransomware (Crypto24 Variants)

A new wave of Crypto24 ransomware variants struck ICT firms and education institutions between February and April. These strains used double-extortion tactics, encrypting critical data while threatening to publicly leak stolen files unless a ransom was paid. One prominent April case involved a Hanoi-based cloud infrastructure provider, which had to shut down services to dozens of SMEs after being infected. The ransomware executables were customized for Vietnamese-language environments and included reconnaissance modules to extract network maps and high-value asset lists before encryption. Victims who refused to pay saw snippets of their internal communications posted on Telegram leak channels.

DDoS Operations

Vietnam faced a dramatic spike in Distributed Denial-of-Service (DDoS) attacks, with over 150 confirmed incidents reported by local ISPs and government CERT teams between January and April. A pronounced surge was recorded in April, coinciding with public protests and regional geopolitical tension. Government portals, education result systems, and municipal utility websites were hit with volumetric traffic floods, some exceeding 60 Gbps. These attacks were often launched using IoT botnets composed of compromised Vietnamese routers and CCTV devices. While most services were restored within hours, some experienced outages lasting over 24 hours due to poor mitigation infrastructure.

Social Engineering & Fake AI Utilities

Cybercriminals leveraged public interest in artificial intelligence to craft highly convincing social engineering campaigns. Dozens of fake Vietnamese-language websites offered free AI chatbot tools, CV optimization platforms, and resume generators — which, when accessed, prompted users to input credentials or

download malware-laced ZIP files. These files commonly contained JavaScript downloaders or malicious Excel macros, which installed info-stealers (such as Lumma Stealer) or lightweight backdoors to facilitate future exploitation. These lures were often spread via social media platforms like Facebook and Zalo, targeting job seekers and students.

CMS Exploits in Media Infrastructure

Vietnamese media platforms running outdated or unpatched Content Management Systems (CMS) such as Joomla and WordPress were heavily targeted during Q1 2025. Attackers exploited plugin vulnerabilities to gain editorial access, alter headlines, inject malicious scripts, and steal unpublished content. The April breach of a state-run media outlet revealed poor CMS maintenance and the absence of multi-factor authentication. Sensitive internal files — including interview scripts and embargoed stories — were exfiltrated and later used in influence operations online. In one case, fake content injected into a news article was briefly propagated by aggregators before takedown.

The techniques observed highlight the increasing tactical diversity among threat actors targeting Vietnam. From mass-scale DDoS and ransomware to socially engineered credential theft and CMS abuse, these incidents underscore the need for multi-layered defense strategies, timely patching, and robust digital awareness among both public and private sector entities.

Cyberattack sophistication ranges from simple to highly complex methods.

05

Incident Timeline (January - April 2025)

Incident Timeline (January - April 2025)

January

Initial low-intensity DDoS attacks were launched by hacktivist group AnonymousVNLBN, targeting lightly defended government portals and public school domains. CERT Vietnam observed early probing and scanning of .gov.vn subdomains and vulnerable university-hosted CMS platforms. No major service disruptions were reported at this stage.

February

Persistent network scans escalated into coordinated denial-of-service attacks on municipal systems, particularly e-learning portals and public health information sites. A Hanoi-based vocational education site experienced over 24 hours of downtime, marking the first significant public impact. The government's cybersecurity center flagged over 400 distinct malicious IPs involved in repeated attacks.

March

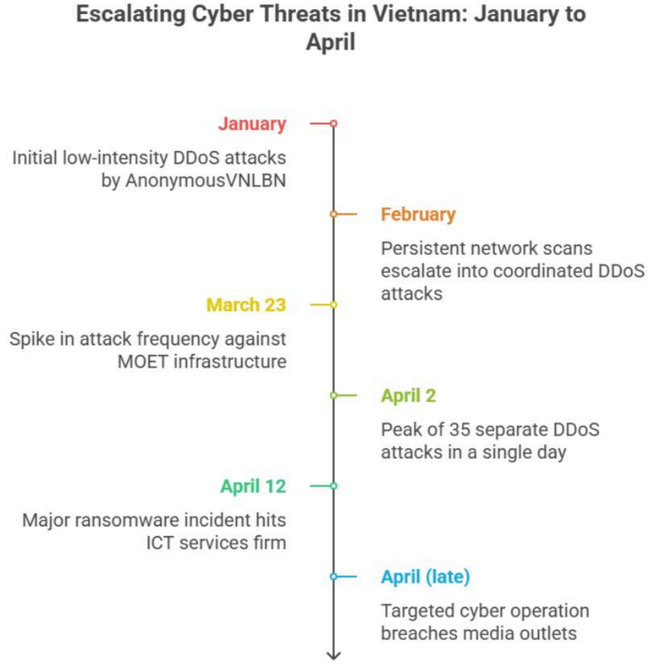
On March 23, a spike in attack frequency was noted, with sustained attacks against MOET (Ministry of Education and Training) infrastructure. This culminated in a peak on April 2, when 35 separate DDoS attacks were logged in a single day, according to the Ministry of Information and Communications (MIC). Botnet traffic traced to compromised routers in both domestic and regional IP ranges.

April (Early)

On April 12, a major ransomware incident hit a top ICT services firm supplying infrastructure to dozens of SMEs and startups. The attack used a Crypto24 double-extortion variant, which encrypted core systems and leaked exfiltrated data via Telegram. Service outages were confirmed across multiple Vietnamese startups reliant on the firm's VPS infrastructure.

April (Late)

A targeted cyber operation breached multiple state-aligned media outlets, gaining editorial access and backend control. Attackers were able to alter headlines and steal sensitive, embargoed materials. Internal investigation suggested exploitation of outdated CMS plugins and poor password management. Some compromised content was briefly circulated on disinformation channels tied to regional influence campaigns.



06
Principal Threat Actors

Principal Threat Actors

Between January and April 2025, Vietnam faced a broad spectrum of cyber threats originating from both regional and international actors. These ranged from politically motivated hacktivists to financially driven ransomware groups and state-sponsored APTs. Several distinct threat actor profiles emerged based on telemetry from Vietnamese CSIRTs, dark web observations, and global threat intelligence platforms.

AnonymousVNLBN

In July 2024, GlobalBank, a multinational financial institution operating in over 50 countries, including Saudi Arabia, was targeted by the BlackCat (ALPHV) ransomware group. The attackers breached a cloud-based third-party service provider, leading to the encryption of critical banking systems and a ransom demand of $80 million in Bitcoin. This attack disrupted transaction processing and ATM operations across multiple regions.

Crypto24-Affiliated RaaS Groups

Ransomware-as-a-Service operators linked to Crypto24, a known double-extortion malware family, were behind the April 12 attack on a major ICT infrastructure firm in Vietnam. These actors offer customized ransomware kits to affiliates on underground forums.

Their attack methods included initial access via compromised RDP and email phishing with malicious Excel macros. Victims received ransom notes in Vietnamese, suggesting local customization of payloads.

APT41 (China-linked)

The China-nexus advanced persistent threat group APT41 was linked to reconnaissance and silent infiltration campaigns against Vietnamese telecom and logistics firms during Q1 2025. Using the DeepData framework, APT41 reportedly targeted fiber backbone providers and undersea cable infrastructure monitoring systems. Indicators of compromise (IOCs) were matched with previous campaigns involving malware loaders like Cobalt Strike and ZxShell. These intrusions were stealthy and long-term, likely focused on espionage rather than disruption.

Earth Estries

A lesser-known but persistent cyber espionage actor, Earth Estries was attributed to long-dwell intrusions in Vietnam's telecom core and national data exchange nodes. Reports by regional threat hunters indicated unusual beaconing patterns from telecom exchanges in Ho Chi Minh City and Da Nang, pointing to ongoing surveillance or data exfiltration. Earth Estries' TTPs (tactics, techniques, and procedures) include fileless malware, custom PowerShell scripts, and use of legitimate admin tools (LOLBins).

Infostealer Syndicates

Vietnamese consumers were hit hard by global info-stealer malware syndicates, especially during the spike in fake AI tool campaigns. Threat actors pushed malware like Lumma Stealer, Vidar, and RedLine through fake ChatGPT, Stable Diffusion, and language translation tool downloads. Victims typically landed on cloned Vietnamese-language sites via paid Google and Facebook ads. Exfiltrated data included browser passwords, crypto wallet credentials, and saved banking logins.

Socks5Systemz Operators

Vietnamese consumer and business endpoints were observed participating — often unknowingly — in the Socks5Systemz proxy botnet, a global network reselling IP bandwidth for malicious purposes. Infected devices were used to anonymize cybercriminal operations, including phishing campaigns and brute-force attacks in other regions. Devices were recruited through free VPNs and mobile APKs disguised as privacy apps or file managers.

These actors reflect the diverse, hybrid threat environment facing Vietnam in 2025 — where cybercriminal, ideological, and geopolitical motivations intersect. Both state and private-sector infrastructure have been placed at risk, and understanding the nature of these actors is key to building targeted defenses.

07

Dark Web & Underground Trends

Vietnam continues to face increased exposure in darknet ecosystems, with local infrastructure, credentials, and user data actively traded or weaponized. Several underground platforms—particularly Russian-speaking forums, Telegram leak channels, and Chinese-language dark markets—have featured Vietnam-centric content, especially following incidents in 2

Ransomware-as-a-Service (RaaS) Listings with Vietnam-Specific Access

RaaS affiliates advertising on forums like RAMP and Exploit began listing access to Vietnamese servers—including RDP credentials and VPN access to ICT providers, education portals, and regional e-commerce backends. These offers often included “domain admin” access and were bundled with “no EDR” environments. Notably, access to a southern Vietnam-based cloud hosting provider was sold just one week before the April ransomware incident involving Crypto24.

Leaked CMS Logins from Media and Government Entities

Vietnamese media houses and provincial government portals using platforms like WordPress, Joomla, and Laravel were disproportionately impacted by CMS credential theft. Threat actors posted verified admin panel logins for news agencies and local municipality sites on forums like BreachForums (prior to its mirror takedown in March 2025). Some credentials were obtained via infostealer logs; others were likely extracted during the April wave of editorial system breaches.

Malware-as-a-Service Kits in Vietnamese Language

Starting mid 2025, underground vendors began promoting localized stealer kits and RATs (Remote Access Trojans) using Vietnamese UIs and social engineering lures. These kits were disguised as AI productivity apps or resume enhancement tools, specifically designed to spread via Vietnamese social networks and Telegram channels. One sample of “AutoGPT Enhancer Pro”, discovered by a Ho Chi Minh City-based infosec firm, contained embedded Lumma Stealer variants.

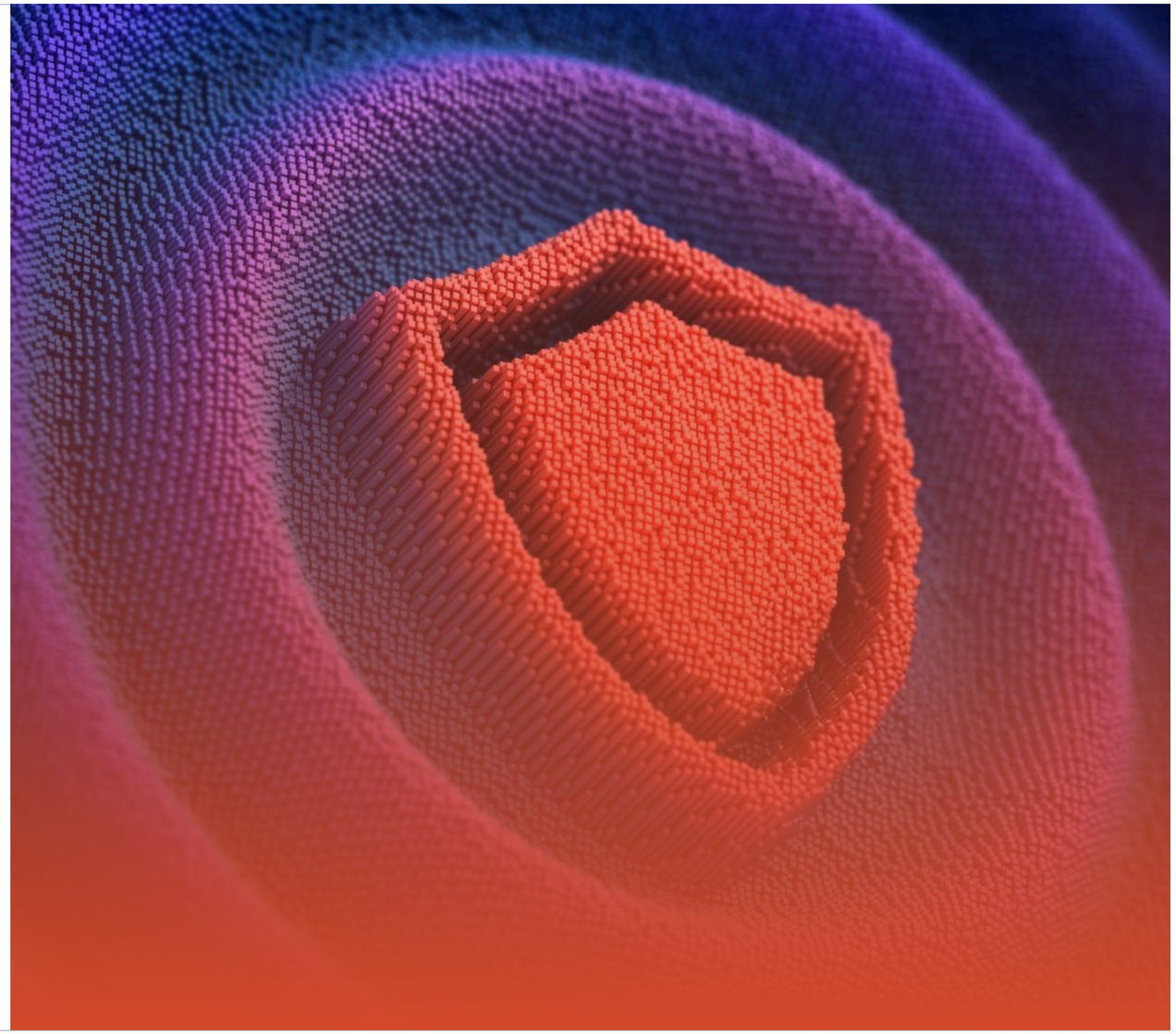
SpyLoan Android Data Dumps on Telegram & Dark Markets

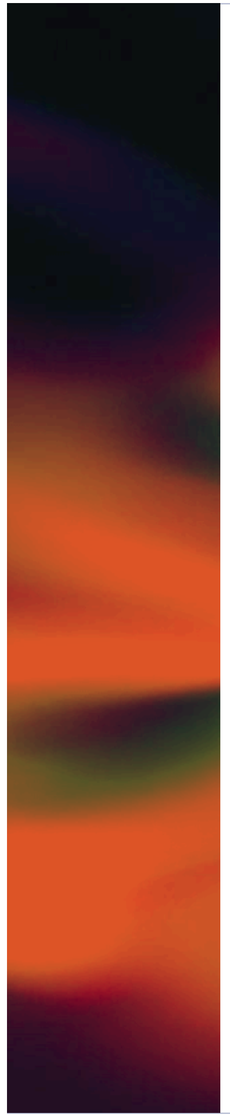
SpyLoan malware continued to wreak havoc in Southeast Asia, and Vietnam remained one of its prime targets. In 2025, analysts identified three Telegram channels that shared Vietnamese user data dumps, including ID scans, contact lists, and geolocation logs — all harvested via rogue loan apps. These channels often cross-posted links to dark markets like Genesis Store clones and Russian marketplaces, offering logs in bulk for as little as $20.

The surge in Vietnamese-focused exploits on dark markets shows how cybercriminal economies are evolving to regionalize their operations. Easy access to local credentials, infrastructure vulnerabilities, and infected mobile devices continues to empower adversaries — especially when paired with affordable MaaS and RaaS services tailored for low-skill operators.

08

Diplomatic & Political Undercurrents





Between January and April 2025, Vietnam experienced cyber operations with clear geopolitical overtones, reflecting the growing strategic interest in its digital and physical infrastructure projects. One particularly sensitive incident involved a targeted cyber-espionage campaign that raised diplomatic alarms and triggered quiet foreign intervention.

Espionage Targeting Infrastructure Deal Involving Western Conglomerate ("Big A")

In Q1 2025, cybersecurity analysts detected a stealthy, high-sophistication intrusion targeting project management networks and encrypted file-sharing portals used by a Vietnamese government ministry and its foreign counterparts. The breach focused on intercepting contract documents, architectural plans, and negotiation details related to a critical smart transit and energy infrastructure project, co-led by a major Western firm referred to here as "big A."

The attackers used:

- **Custom malware loaders** with rootkit capabilities to maintain persistence,
- **Tunneling through telecom backbone nodes** for covert data exfiltration,
- **Encrypted backchannels over SSH and DNS,** suggesting state-level operational tradecraft.

Though no formal attribution was made, technical overlap with past East Asia-linked APT campaigns, along with the operation's geopolitical focus, led to quiet diplomatic dialogue. This included:

- **Private security briefings** between Vietnam's Ministry of Public Security and select foreign embassies,
- **Tech envoy engagement** by the affected Western nation to discuss counter-surveillance support,
- **Increased scrutiny** over international procurement processes and cloud infrastructure hosting locations.

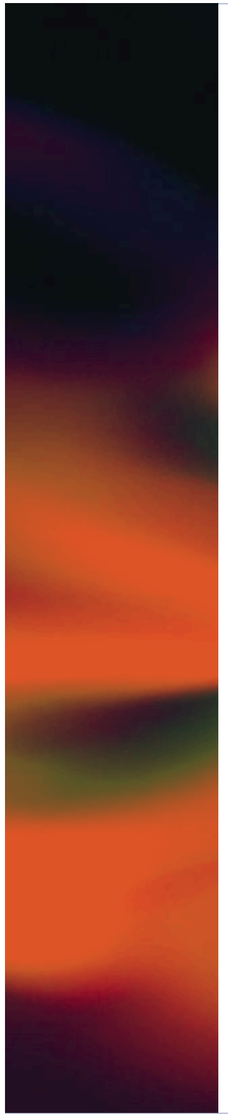
Implications for Vietnam's Geostrategic Cyber Posture

This operation underscores how cyber tactics are now being embedded into broader diplomatic maneuvering in Vietnam's increasingly multipolar economic environment. With the country actively deepening both Eastern and Western technology alliances, it is likely that cyber-espionage targeting trade, infrastructure, and defense planning will escalate in complexity and sensitivity through 2025 and beyond.

09

Recommendations for Enhancing Resilience

Recommendations to Enhancing Resilience



To respond effectively to the wave of cyberattacks witnessed in early 2025 especially those impacting government portals, ICT providers, and media entities—Vietnam must prioritize a proactive, cross-sector cybersecurity strategy.

Policy & Regulation

Enforce Mandatory Breach Reporting (72h Rule):
Despite being outlined in Vietnam's 2022 Cybersecurity Decree, breach reporting remains inconsistent. Regulators should compel both public and private organizations—especially in ICT and critical infrastructure—to report breaches within 72 hours, enabling faster incident containment and coordinated national responses.

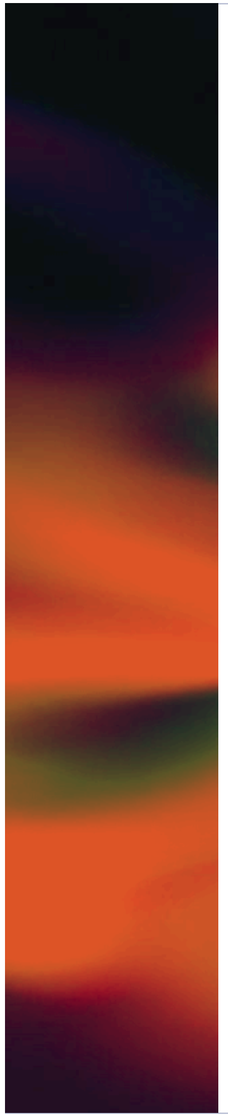
Mandate Audits of CMS and Government Portals:
Given the media-related breaches in April 2025, annual audits of editorial and content management systems should be conducted by licensed third parties. This applies especially to platforms used by state-linked media and ministries, which are often soft targets for both political actors and criminal groups.

Technical Controls:

Adopt Zero Trust Architecture for Public Systems:
With attackers exploiting lateral movement in flat networks, zero trust segmentation should be adopted across public-sector IT, telecom carriers, and utilities. Access should be limited based on verified identity, least privilege, and continuous monitoring.

Implement Multi-Factor Authentication and Endpoint Detection (EDR):
Most successful breaches exploited poor credential hygiene. Organizations must enforce MFA across all services, particularly for admin panels, remote access tools, and payment portals. Deploying next-gen EDR solutions will also improve threat detection and limit ransomware propagation.

Maintain Offline, Immutable Backups:
The Crypto24 ransomware campaign in April crippled several ICT environments due to lack of offline backups. Agencies and companies must maintain regular, immutable backups disconnected from core infrastructure to ensure restoration capabilities after encryption or wiper attacks.



Awareness & Training

Launch Nationwide Phishing Awareness Campaigns: Widespread phishing and smishing attacks exploiting fake government links (e.g., eCitizen, tax agencies) call for urgent grassroots awareness efforts. These campaigns should be broadcast via SMS, social media, and radio, and localized in Vietnamese dialects.

Specialized Security Training for Media and ICT Staff: Given the exploitation of CMS systems and editorial accounts, frontline media professionals and ICT service staff must receive targeted training. Focus areas should include secure software usage, endpoint hardening, phishing detection, and account hygiene.

Threat Intelligence Sharing

Improve Collaboration Between National and Sectoral CERTs: Vietnam's A05, VNCERT, and law enforcement agencies must deepen their collaboration with banking, telecom, and ICT sector ISACs, ensuring real-time sharing of indicators of compromise (IOCs), attack TTPs (tactics, techniques, procedures), and dark web findings.

Regional Cooperation via Southeast Asian CERT Networks: Vietnam should actively exchange threat intelligence with regional counterparts, especially through ASEAN-SingCERT and ThaiCERT. Cross-border ransomware groups and infostealer syndicates often operate regionally, so real-time intelligence exchange is vital.

By enforcing these measures, Vietnam can significantly reduce its cyber risk exposure and build a more resilient national cyber ecosystem—especially ahead of the 2027 elections and deepening digital reliance.

Conclusion: Securing Vietnam's Digital Future

Vietnam's cybersecurity environment between January and April 2025 was marked by a significant escalation in both the volume and sophistication of cyber threats. From politically motivated DDoS campaigns and ransomware targeting ICT infrastructure, to media platform breaches and deep cyber-espionage linked to foreign interests, the country faced a multi-vector threat landscape.

As Vietnam continues to position itself as a digital and economic hub in Southeast Asia, its telecom infrastructure, public institutions, and media platforms have become high-value targets. Hacktivists, cybercriminal syndicates, and state-aligned advanced persistent threats (APTs) have all played active roles in undermining service continuity, trust, and data integrity.

Conclusion: Securing Vietnam's Digital Future

Key challenges identified include:
· Inconsistent patching and segmentation across public-sector systems,
· Limited threat detection capabilities among SMEs and regional entities,
· Gaps in awareness, especially among media and mobile users vulnerable to phishing and malware-laced apps.

To counter these growing threats, Vietnam must:
· Enforce robust cybersecurity regulations including breach disclosure and system audits,
· Accelerate adoption of Zero Trust architecture and endpoint protection, especially in critical sectors,
· Promote nationwide cyber hygiene education, extending to rural and lower-literacy populations,
· Deepen real-time threat intelligence sharing across ASEAN and public-private stakeholders.

Without coordinated action, Vietnam risks becoming a persistent soft target in the geopolitical and cybercrime crossfire. However, with the right strategic investments, Vietnam can harden its defenses, maintain public trust, and assert digital sovereignty in an increasingly contested cyberspace.