DARKTRACE

ANNUAL THREAT REPORT 2026: APJ REGIONAL OUTLOOK

The global cyber threat landscape in 2025 was increasingly defined not by uniform trends, but by regional threat economies shaped by maturity, geopolitics, the speed of digitization, and attacker objectives. This regional breakdown provides a focused analysis of the key threat trends, notable threat actors, and outlook for the APJ region.

The APJ region is undergoing rapid digital transformation, driven by large-scale adoption of cloud services, 5G connectivity, and AI integration. These advancements, while enabling innovation, introduce significant challenges around data sovereignty, misconfigurations, and legacy system vulnerabilities.

Geopolitical tensions, such as the South China Sea dispute, strained Democratic People's Republic of Korea (DPRK)-Republic of Korea (ROK) relations, and global conflicts fuel state-sponsored cyber campaigns and disinformation operations.

Fragmented regulatory frameworks and uneven cybersecurity maturity across economies amplify exposure, leaving critical infrastructure, financial institutions, and government entities particularly vulnerable to ransomware, phishing, and AI-powered attacks.

REGIONAL TRENDS AND STATISTICS

84% of APJ organizations agree that AI-powered cyber threats are already impacting them and will continue to do so.

Only 42% of APJ organizations have a formal policy for safe AI use, and confidence in traditional solutions has fallen 14 points; 55% now say those tools don't adequately stop AI-powered attacks (up from 41% in 2024).

Phishing targeting pattern: In APJ, 14% of phishing emails target VIP users significantly lower than the global 25%, indicating broader, organization-wide phishing rather than VIP-heavy campaigns.

Source: Darktrace's APJ Threat Landscape Report

NOTABLE THREAT ACTORS

Actor	Motivation & Targets	Key Tactics
Lazarus Group (DPRK-linked)	Strategic espionage; financial gain targeting RoK government, defense, and cryptocurrency firms	**Spear phishing** (T1566) **Supply-chain exploits** (T1195)
APT40 (China-nexus)	Espionage aligned with The Belt and Road Initiative (BRI); targets Southeast Asian Governments, Telecommunications, Australia, Japan	**Exploit public-facing apps** (T1190) **Spear phishing** (T1566) **Encrypted webshells** (T1505.003)
MirrorFace (Earth Kasha)	Espionage targeting Japanese media, political organizations, research institutions	**Spear phishing** (T1566) **Malware deployment** (T1204.002)
Mustang Panda	Espionage including against Southeast Asian law enforcement agency.	**Spear phishing** (T1566) **Remote Access Tool** (T1219) **Registry persistence** (T1547) **LOTL techniques** (T1059.001)

CASE STUDY: Mustang Panda

In February 2025, Darktrace researchers identified a Mustang Panda campaign targeting the Royal Thai Police to deliver the Yokai backdoor. The initial file was a RAR archive named "ด่วนมาก เชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร FBI.rar (English: Very urgent, please join the cooperation project to train the FBI course.rar)".

While the initial access vector is unknown, it was highly likely delivered via phishing email. Inside the archive was an LNK shortcut file, ด่วนมาก เชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร FBI.docx.lnk, a disguised PDF file, and a folder named $Recycle.bin. The shortcut file executes ftp.exe, which then processes the commands embedded in the disguised PDF file as an FTP script, an automated sequence of FTP commands. The installed payload, PrnInstallerNew.exe, is a maliciously altered version of legitimate PDF printer software. It employs detection-evasion techniques by dynamically constructing and invoking system functions at runtime rather than referencing them directly, making its behavior more difficult for security tools to analyze.

บันทึกข้อความ

ส่วนราชการ บก.อก.บช.ก. **โทร.** ๐ ๒๑๙๓ ๙๓๙๓

ที่ ๐๐๒๓.๑๑๔/ **วันที่** ธันวาคม ๒๕๖๗

เรื่อง ขอเชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร การป้องกันและปราบปรามอาชญากรรมข้ามชาติ บริเวณชายแดนไทย

เรียน ผบก.ป.

รอง ผบก.ป.

ผกก. ในสังกัด บก.ป.

เพื่อโปรดทราบ

รองผกก. ถึง รอง สว. ในสังกัด บก.ป.

ด้วยในปี ๒๕๖๗ ปัญหาอาชญากรรมข้ามชาติในไทยยังคงปรากฏต่อเนื่องและส่งผลกระทบต่อความมั่นคงในวงกว้าง เนื่องจากการพึ่งพาการสื่อสารทางออนไลน์และการทำธุรกรรมผ่านระบบอินเทอร์เน็ตที่เพิ่มขึ้น ส่งผลให้อาชญากรรมหลายประเภทขยายตัว เฉพาะอย่างยิ่งอาชญากรรมที่เชื่อมโยงกับกลุ่มบุคคลต่างชาติในพื้นที่ชายแดนประเทศรอบบ้านไทย อาทิ การค้ามนุษย์ การฉ้อโกงผ่านโครงข่ายอินเทอร์เน็ต การผลิตและจัดหาเอกสารปลอม เป็นต้น

ดังนั้น บก.อก.บช.ก กำหนดจะชวนเชิญจนท.อาวุโสด้านงานปราบปราม จากสำนักงานสอบสวนกลางสหรัฐอเมริกา (FBI) ร่วมมือจัดการฝึกอบรมหลักสูตร การป้องกันและปราบปรามอาชญากรรมข้ามชาติ บริเวณชายแดนไทย

จึงให้ บก.ป. พิจารณาจัดหาข้าราชการตำรวจที่เกี่ยวข้อง เข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตรฯ บก.อก.จะแจ้งกำหนดการ เวลาและสถานที่ ในโอกาสแรก หลังประสานกับฝ่ายสหรัฐฯเสร็จ

จึงเรียนมาเพื่อโปรดทราบ

Figure 01: Decoy docx file ด่วนมาก เชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร FBI.docx. (English: Very urgent, please join the cooperative training project for the FBI course.docx)

After resolving its API calls, the malware connects to its command-and-control (C2) server over port 443, sending the hostname and awaiting further instructions. To maintain persistence, it adds itself to the user's startup registry, ensuring it executes each time the user logs in.

CASE STUDY: Wazuh Exploit

In 2025, attackers exploited an unsafe deserialization vulnerability in Wazuh Manager (CVE-2025-24016), enabling remote code execution.

This allowed adversaries to deliver Mirai botnet payloads across Internet of Things (IoT) devices, leveraging compromised systems for large-scale botnet attacks. The Wazuh exploit enabled Mirai botnet spread across IoT devices, creating risks of operational disruption and supply chain impact. This highlights the need for timely patching of vulnerable platforms, strict network segmentation, and limiting remote access tools. Organizations should also leverage AI-driven detection to spot anomalous activity early and reduce dwell time.

CASE STUDY: Gh0stRAT

In May 2025, attackers deployed the remote access trojan Gh0stRAT against a customer in the APJ region. Initial activity involved connections to a suspicious domain, which subsequently triggered repeated executable downloads from a rare IP address associated with the Hong Kong-based hosting provider AS138995 Antbox Networks Limited.

The frequent abuse of hosting providers within the APJ region enables malicious C2 traffic to blend more easily with legitimate network activity common among APJ-based organizations. To counter this, organizations should leverage AI-driven detection capable of identifying anomalous external connections that may represent C2 communication—regardless of geographic location.

GOVERNMENT & REGULATORY OVERVIEW

Governments across APJ are tightening cybersecurity laws to address rising threats and AI risks:

Japan's **Active Cyber Defense Act** will come into effect 2026, enabling preemptive action and mandatory reporting for critical infrastructure, alongside SME-focused awareness programs.

RoK introduced an overarching **Framework Act on AI,** enforced in January of 2026, aimed at curbing the misuse of generative AI, and strengthened privacy through the Personal Information Protection Act, most recently amended in 2023, while shifting to a proactive national defense strategy.

Australia launched the **Cybersecurity Act (2024)** with ransomware payment reporting and adopted global standards for Operational Technology (OT) and AI security.

Across Southeast Asia, Association of Southeast Asian Nations (ASEAN) initiatives like the Cybersecurity Cooperation Strategy and Singapore's planned Digital Infrastructure Act aim to secure cloud ecosystems and critical digital infrastructure.

INSIGHTS & OUTLOOK

Organizations in APJ continue to face persistent vulnerabilities stemming from misconfigurations, phishing, and insider risks.

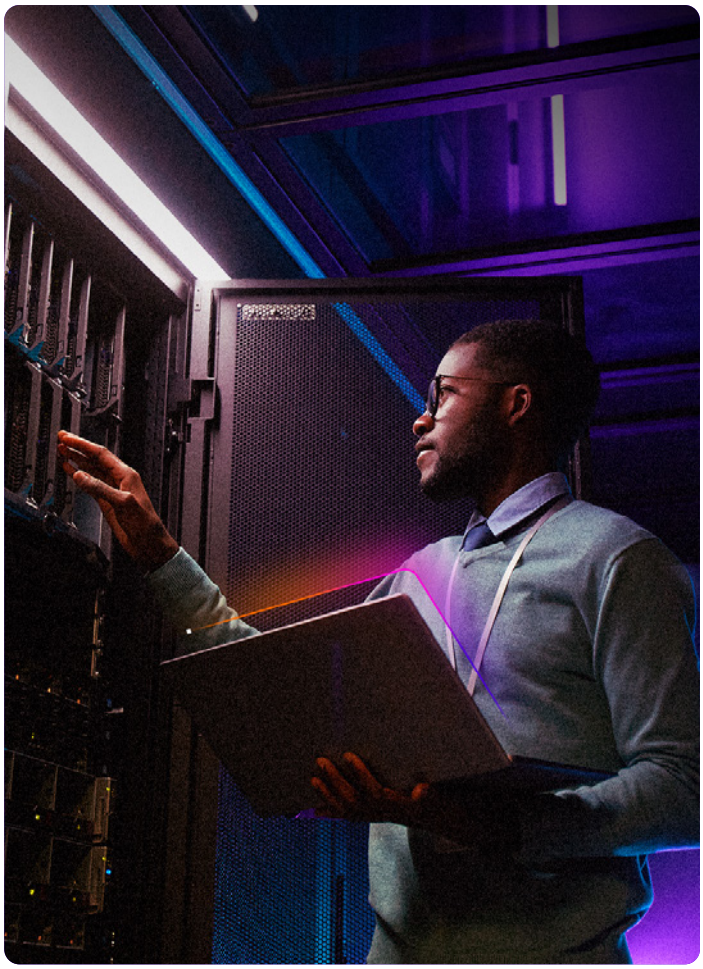
AI-driven attacks are on the rise, enabling more sophisticated phishing and accelerating malware development.

At the same time, hybrid cloud environments and increasing IT-OT integration are expanding the regional attack surface, while fragmented regulations and reliance on legacy systems contribute to systemic weaknesses.

Looking ahead, the region is likely to see continued growth in AI-powered phishing and identity abuse, along with a rise in attacks targeting critical infrastructure and OT systems. Regulatory attention on AI and cloud security will intensify, though enforcement is expected to remain inconsistent across APJ.

REGIONAL ANALYSIS METHODOLOGY:

It is important to note that while the analysis is relevant and broadly representative of wider global trends, it is also influenced by the geographic distribution of Darktrace's customer base. For example, within the Americas (AMS) region, the US represents the largest share of Darktrace customers, meaning insights in this section may be weighted more heavily toward US-based activity.



North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com