pwc

Case studies

The new shape of cyber risk in Malaysia: AI, quantum, and trust

May 2026

Malaysian organisations stand at a critical inflection point as artificial intelligence (AI) accelerates the sophistication of cyber threats and attacks become identity driven. What does resilience mean in this threat landscape?

The way organisations are being compromised is changing, and the shift is quieter than most expect. Attackers are no longer breaking down doors; they are logging in, exploiting trusted identities and moving through systems as though they belong there.

At the same time, the tools available to both the attackers and the defence are evolving. As noted in **PwC's Annual Threat Dynamics 2026** report, AI is reshaping how attacks are launched and how they are detected. Blind spots across edge devices, supply chains and cloud ecosystems are increasingly being tested, not through brute force, but by turning trusted dependencies into pathways.

For Malaysia, this is not a distant concern. The country's rising international profile—from its Tier 1 ranking in the ITU Global Cybersecurity Index and regional leadership on ASEAN cybersecurity policy, to its proactive push on post-quantum cryptography (PQC)—brings greater visibility. And visibility brings attention. As reported in PwC's 2026 Global Digital Trust Insights, escalating geopolitical tensions have prompted 67% of Malaysian business leaders to increase cyber investment, while threats against national critical information infrastructure (NCII) sectors continue to grow.

Three recent cases, spanning different geographies and industries, illustrate these patterns in practice and offer lessons that are directly relevant to organisations operating in Malaysia today.

Authors

Alex Cheng
Director,
Cyber Threat Operations,
PwC Malaysia

Cindy Lee
Senior Associate,
Cyber Threat Operations,
PwC Malaysia

Case study

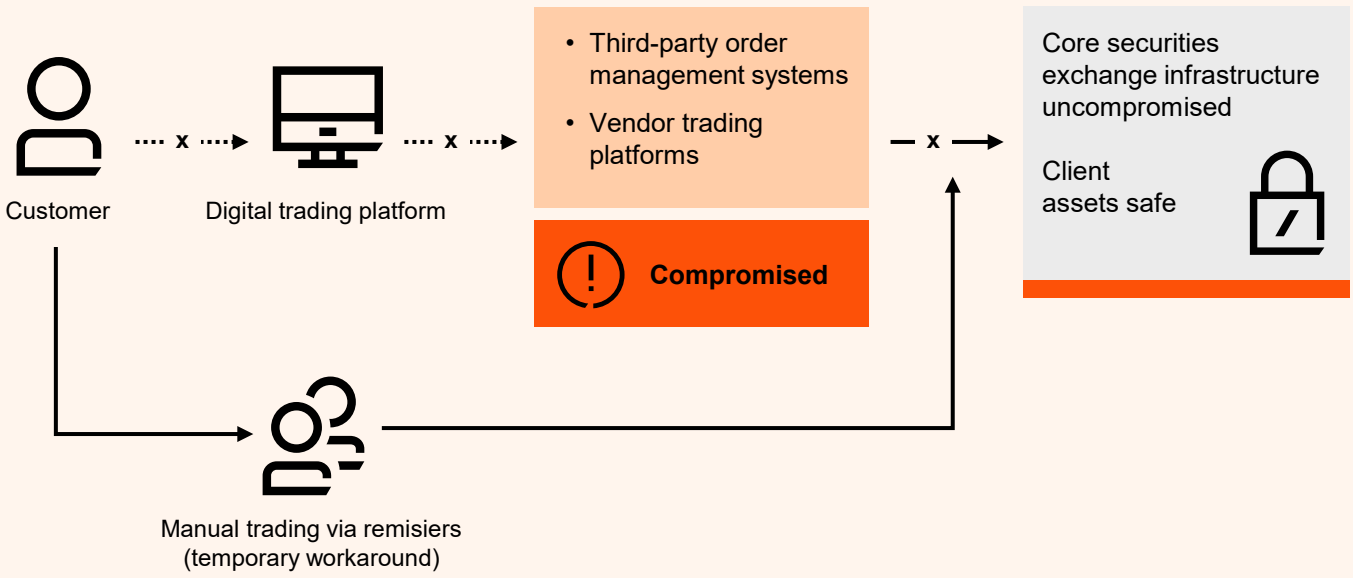
1

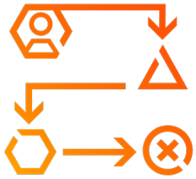
Security breach in third party systems disrupted Malaysia's stockbroking sector

In March 2026, the Malaysian stockbroking sector experienced not just one, but two separate incidents of significant disruptions affecting multiple trading platforms. Both outages lasted several days and temporarily hindered customers' ability to execute trades through their usual digital channels. During these disruptions, customers were advised to place trades manually through remisiers.

Although limited details were disclosed publicly, investigations indicated that both incidents were linked to vulnerabilities in third-party order management systems and vendor trading platforms. In response, some trading platforms took extensive safeguard measures such as suspending trading activities for multiple days and mandating password changes for all clients to ensure all sensitive information are secure after the incidents.

Despite the broker-level disruptions, the core securities exchange infrastructure remained uncompromised. Client assets, including cash balances and securities held in custody, were preserved intact and segregated in accordance with regulatory requirements. Trading in selected international markets continued without interruption throughout the incidents.





Impact of disruptions from the customer's point of view

- Trading suspended or delayed, leading to potential loss of returns
- Mandatory password reset creates inconvenience

Case study

2

Axios npm: How a trusted software package was briefly turned malicious

In March 2026, the popular Axios npm package, commonly used for making requests to REST API endpoints, fell victim to a supply chain attack that led to two malicious versions being published online. Rather than exploiting technical flaws in the package's infrastructure, the attackers took a different route during this attack: **they socially engineered the lead developer of the Axios project to obtain credentials** to the package's repository.

The initial compromise: Identity theft through social engineering

- Convinced the lead developer of the project to join a Slack workplace, carefully crafted after a legitimate company.
- Realistic branding, fake company profiles, makeshift open-source maintainers, and channels sharing LinkedIn posts were used to make the site more convincing.
- The attackers then invited the developer to an online meeting. Several fake participants were involved in the call to make the meeting seem authentic and coordinated.
- During the online meeting, the lead developer was persuaded to download a remote access trojan (RAT) disguised as a software update, with the pretence that their workstation was out of date.
- From the installed RAT, the attackers gained access to the developer's npm credentials.

While there were no public confirmations that deepfake or AI-enabled social engineering techniques were used in this incident, the affected developer noted similarities to social engineering patterns previously attributed to the North Korean threat actor group UNC1069. The group is known for using AI-enabled tactics such as deepfake to convince targets into deploying malware into their system.

Supply chain attack compromise: Distribution of compromised Axios npm package versions

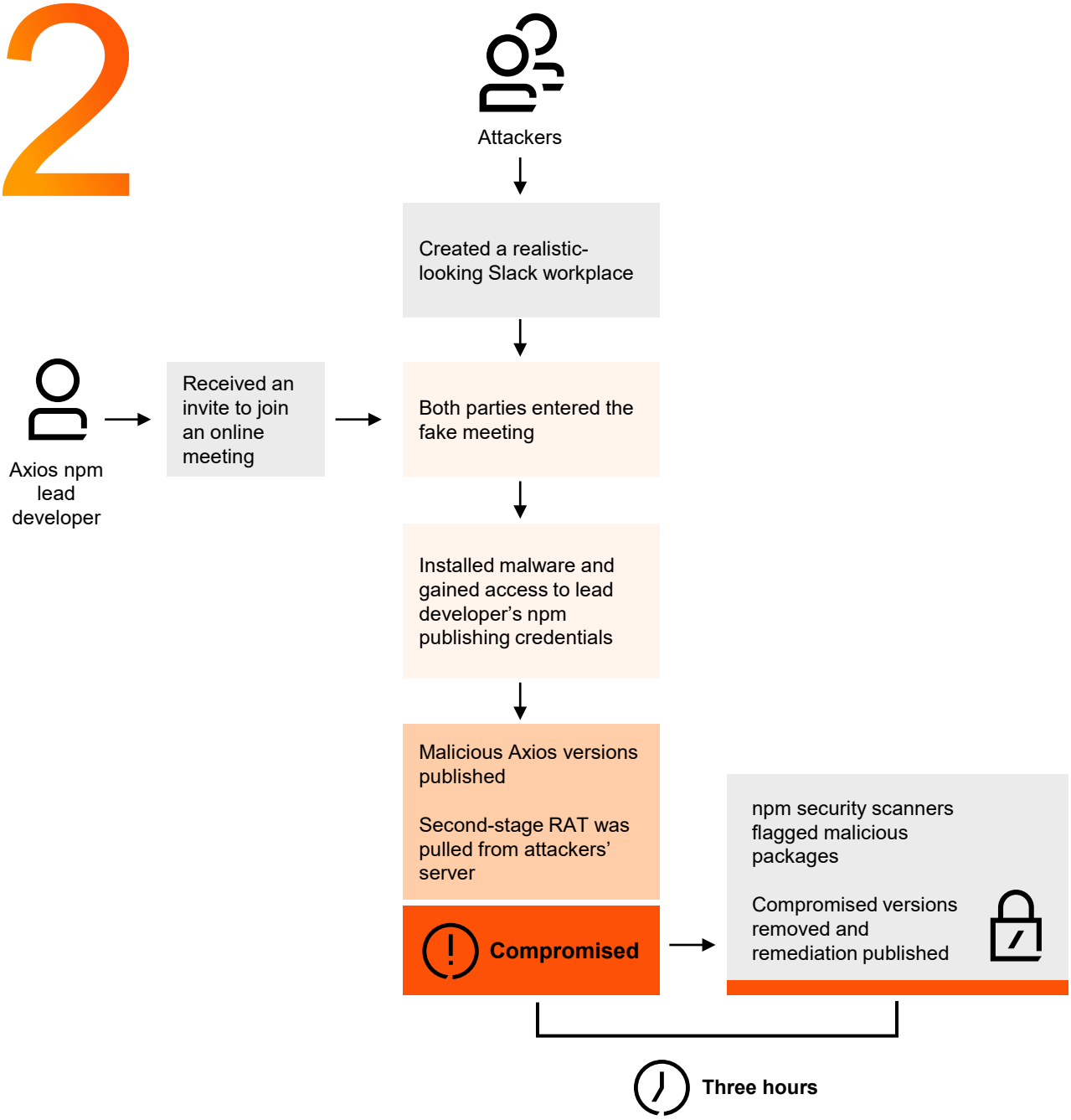
- Using the obtained credentials, the attackers pushed compromised versions of the Axios package into the npm repository.
- The compromised versions contained a hidden dependency (plain-crypto-js) which downloaded a more advanced remote access trojan (a second-stage RAT) from the attacker's C2 server, allowing attackers to execute arbitrary PowerShell code, enumerate directories and files, and inject binary payloads.
- To evade detection, the attackers relied on techniques that minimises on-disk artefacts such as in-memory execution, temporary files, and encoded payloads.

The compromised versions were live for about three hours before it was taken down after being flagged by automated npm security scanners. Following the incident, remediation actions for infected systems and improvements to the maintainer environments were published to ensure that the RAT was removed and to reduce the likelihood of similar incidents from recurring.

Case study

Axios npm: How a trusted software package was briefly turned malicious

2



Impact of disruptions from the customer's point of view

- The compromise impacted individual developer laptops as well as CI/CD pipelines, increasing exposure to downstream supply chain risks
- Disruption to normal development and operational workflows

Case study

3

LiteLLM: A minutes-long supply chain attack with widespread, cascading impact

The LiteLLM supply chain compromise in March 2026—part of a broader campaign by Group TeamPCP—was yet another example that highlighted the dangers of implicit trust in third-party and open-source components.

The attack began with the compromise of the open-source vulnerability scanner Trivy, which served as the initial entry point. Using stolen continuous integration and continuous delivery (CI/CD) credentials from the LiteLLM CI/CD pipeline, the attackers published two malicious LiteLLM versions to the PyPI repository, each containing a sophisticated three-stage payload:

Stage 1:

Harvested over 50 types of credentials, secrets, and keys. Harvested credentials were encrypted and transmitted to a spoofed domain.

Stage 2:

Utilised a toolkit to enable lateral movement within Kubernetes clusters, compromising entire clusters beyond the initially infected system.

Stage 3:

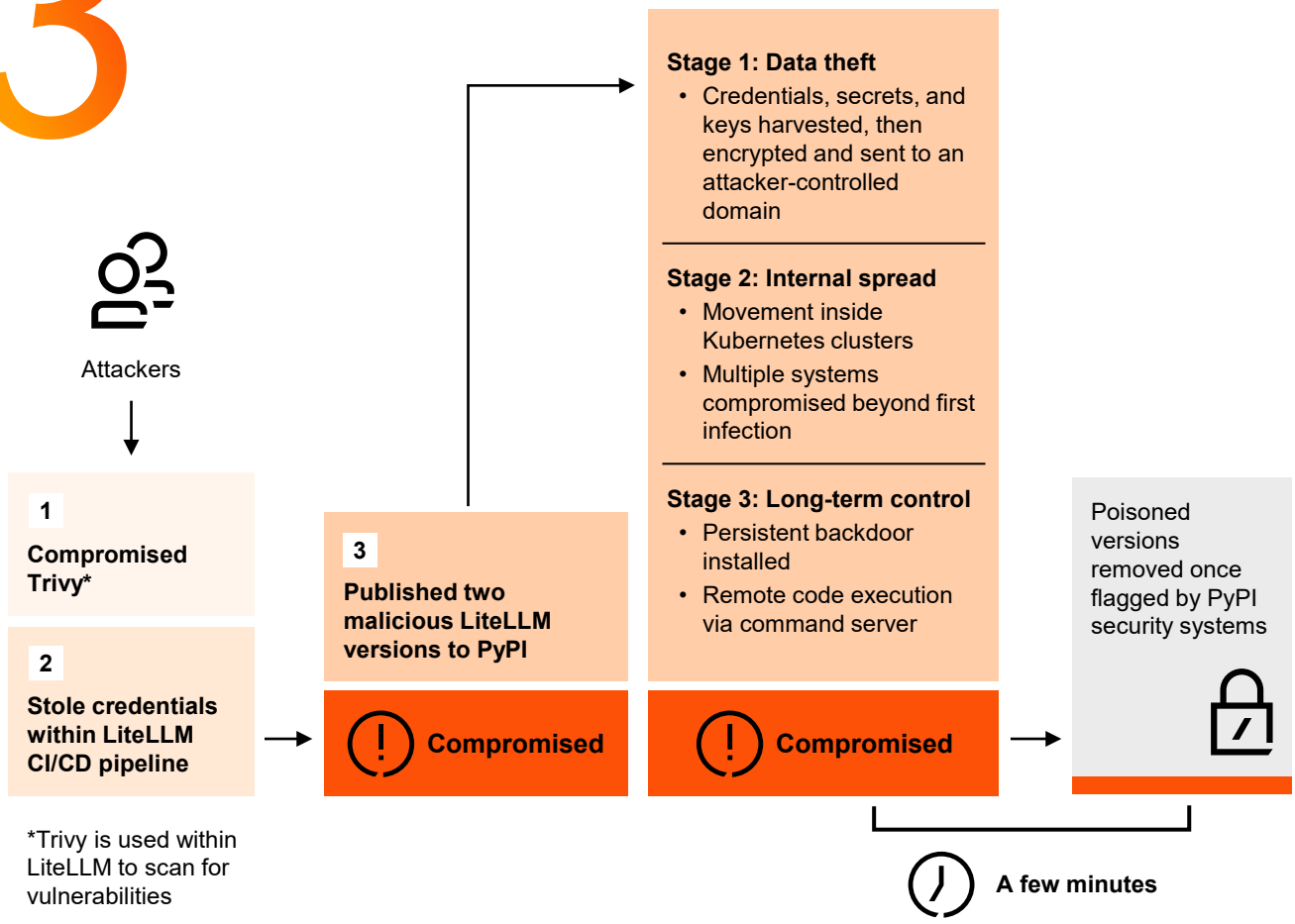
Established a persistent backdoor that allowed remote code execution and maintained long-term access, polling a command-and-control server at regular intervals to retrieve and execute secondary payloads.

Although the poisoned versions were promptly removed within minutes, the damage was already done—tens of thousands of downloads had occurred, causing widespread impact.

Case study

LiteLLM: A minutes-long supply chain attack with widespread, cascading impact

3



Impact of disruptions from the customer's point of view

- Customers' credentials, secrets, and keys harvested, putting their security at risk
- Ongoing projects using the compromised version of LiteLLM had to be halted, causing significant delays and operational disruptions

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

Contact us

Clarence Chan
Partner,
Digital Trust and
Cybersecurity Leader,
PwC Malaysia
clarence.ck.chan@pwc.com

Alex Cheng
Director,
Cyber Threat Operations,
PwC Malaysia
alex.ct.cheng@pwc.com

Tanvinder Singh
Director,
Cyber and Forensic,
PwC Malaysia
tan.singh@pwc.com