ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 2/25 (February)

In Review: Cybersecurity Trends and Challenges In 2024

INTRODUCTION

1. The year 2024 witnessed a significant escalation in cyber incidents, impacting organisations across various sectors. Organisations faced an evolving threat landscape driven by sophisticated cybercriminals that leverage advanced technologies, such as artificial intelligence-powered malware. The expanding attack surface, fuelled by remote work, cloud computing, and the Internet of Things (IoT), further increased vulnerabilities.

2. Notably, the global average cost of a data breach reached US$4.88 million, marking a 10% increase from the previous year. Additionally, nearly 45% of employed individuals worldwide reported falling victim to some form of cyberattacks or scams, compromising personal information such as banking or email accounts. These statistics underscore the growing sophistication and frequency of cyber incidents, necessitating enhanced security measures and proactive strategies.

KEY CYBERSECURITY TRENDS AND CHALLENGES IN 2024

3. Rise of Ransomware Attacks. Ransomware continued to be a predominant threat in 2024, with attackers targeting critical infrastructures, financial institutions, and healthcare systems. The Change Healthcare ransomware attack by the ALPHV/BlackCat ransomware group in February 2024 disrupted the largest healthcare payment system in the United States. This affected numerous healthcare providers and patients, and led to a US$22 million ransom payment.

Other ransomware groups also executed devastating attacks across multiple sectors. For instance, Hades (formerly Conti) group breached HealthCorps, compromising 5.6 million patient records, highlighting ongoing threats to healthcare; the Dark Angels group launched a major attack demanding a US$75 million ransom, demonstrating increasing financial extortion tactics. These incidents highlight the urgent need for robust defences against ransomware, including zero-trust architectures, enhanced endpoint protection, and rapid incident response capabilities. Implementing network segmentation, air-gapped backups, multi-factor authentication (MFA), and continuous security monitoring can help mitigate risks.

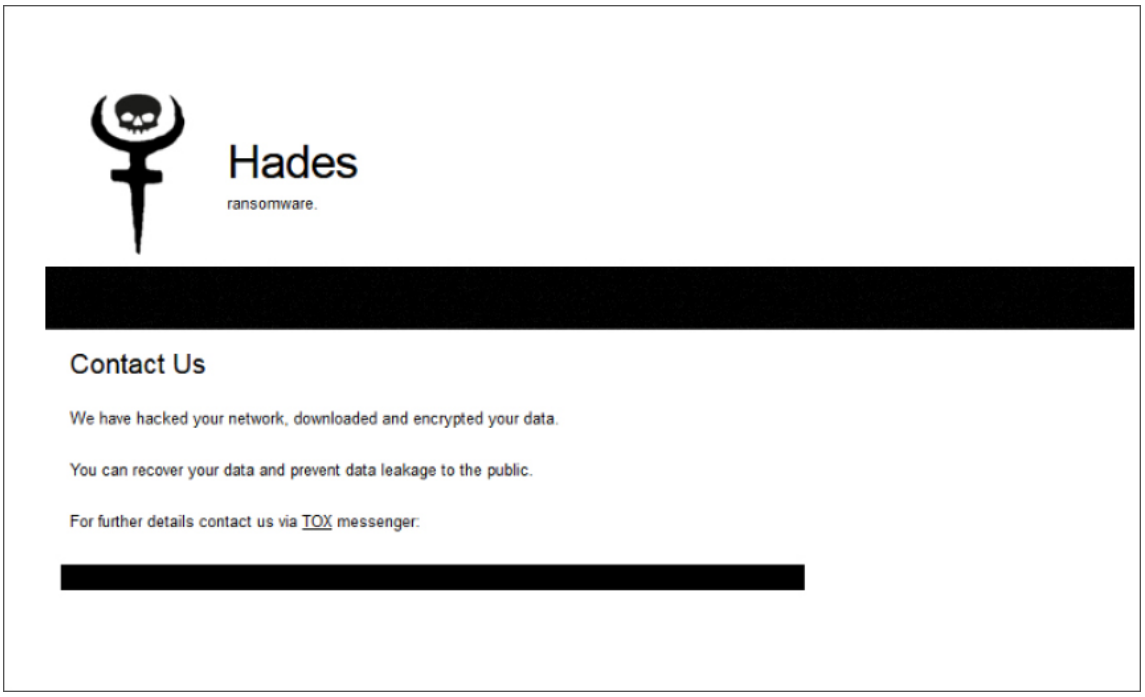

Fig. 1: Example of Hades Ransom Note

4. Increased Third-Party Risk. Cybercriminals increasingly targeted vulnerabilities in third-party vendors to infiltrate organisations. A notable example is the widespread compromise of Ivanti's Connect Secure VPNs, which affected multiple US government agencies and private enterprises. Attackers also targeted open-source software repositories, injecting malicious code into widely used packages. The MOVEit Transfer breach also exposed critical security gaps, which led to extensive data exfiltration incidents worldwide. These incidents reinforce the importance of rigorous third-party risk management and proactive vulnerability patching. This trend emphasises the importance of securing third-party relationships, conducting regular audits, enforcing stricter cybersecurity

compliance among vendors, and enhancing software bill-of-materials (SBOM) practices.

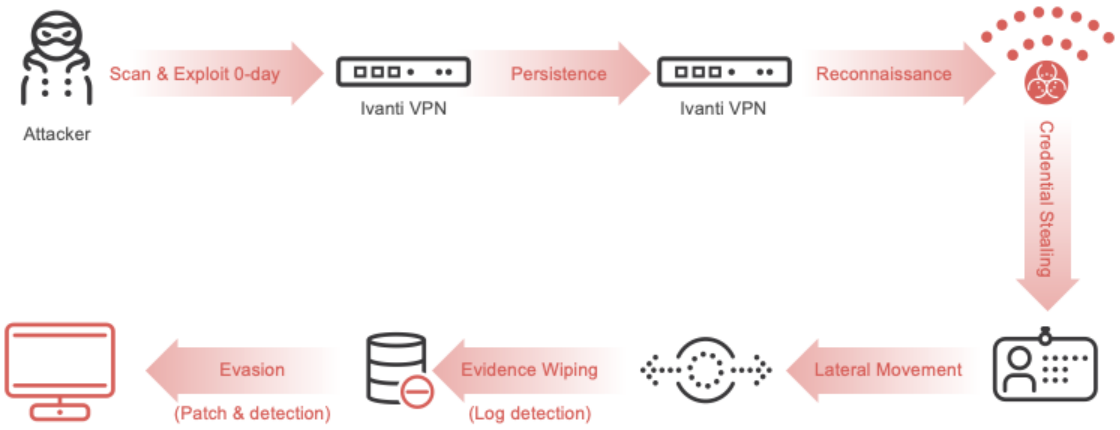

Fig. 2: Ivanti VPN Vulnerabilities Attack Chain

5. Prolonged Recovery Times from Cyber Incidents. Organisations faced extended recovery periods following cyber incidents. Reports revealed that businesses reported taking an average of 7.8 months to recover from cybersecurity breaches – 28 per cent longer than expected and almost two months past the anticipated timeline of 6.1 months. Additionally, severe data exfiltration cases left companies struggling to mitigate reputational damage and financial losses. As cyber insurance premiums surged and coverage requirements became stricter, companies had to rethink business continuity strategies and adopt proactive risk mitigation measures.

6. Exploitation of Emerging Technologies. Cyber adversaries leveraged emerging technologies, such as artificial intelligence (AI), to enhance the sophistication of their attacks. AI-driven phishing and deep-fake fraud became significant concerns, with phishing emails surging by 1,265% since late 2022. Hackers increasingly automated social engineering attacks, making scams harder to detect.

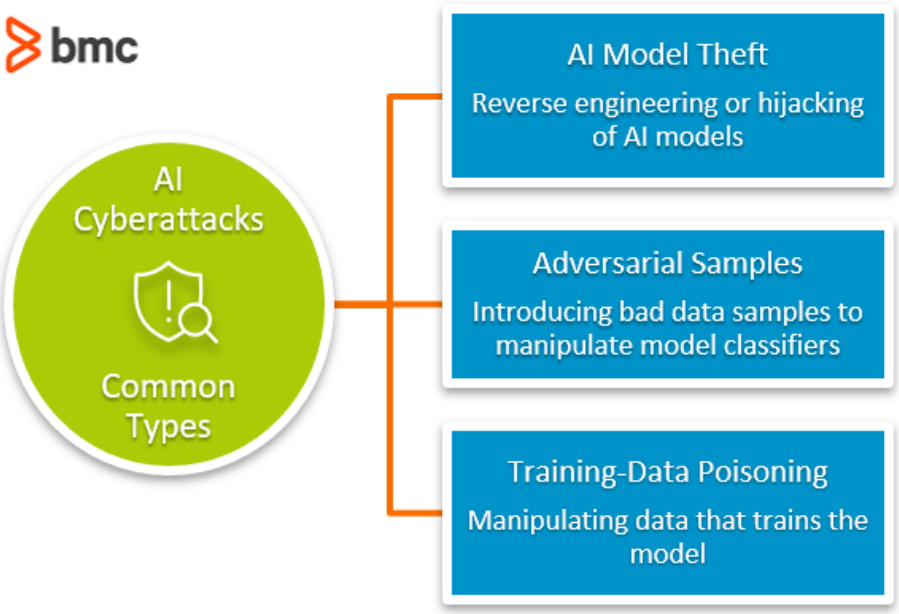

Fig. 3: Common Types of AI Cyberattacks

7. Human Errors and Malicious Insider Threats. Human factors remained a critical vulnerability. 68% of cybersecurity breaches involved a non-malicious human element, like a person falling victim to a social engineering attack or making an error. The CrowdStrike incident in July 2024, where a software update caused widespread system crashes, exemplifies the impact of internal mishaps on organisational security. Insider threats continue to create vulnerabilities within organisations, such as disgruntled employees who may have acted with malicious intent to steal data, disrupt systems, or collaborate with external attackers for personal, financial, or competitive gain. Addressing this challenge requires comprehensive training, stringent internal controls, identity and access management (IAM) solutions, and proactive monitoring of insider threats.

8. Tighter Regulations and Compliance in the Cyber Landscape. Governments and regulatory bodies tightened cybersecurity compliance requirements in 2024. The European Union's NIS2 Directive, the US SEC cybersecurity disclosure rules, and China's Network Data Security Management Regulations imposed stricter reporting mandates, supply chain security measures, and data protection standards. Organisations had to invest in continuous compliance monitoring, risk assessment frameworks, and proactive engagement with regulators to avoid penalties and maintain operational resilience.

THE WAY FORWARD FOR 2025

9. To effectively combat the evolving cybersecurity landscape, organisations could consider the following strategies in 2025:

a. Enhanced Incident Response Planning.

i. Develop and regularly update incident response plans to ensure swift recovery from cyber incidents.

ii. Conduct frequent tabletop exercises to improve response readiness.

b. Supply Chain Security.

i. Implement rigorous security assessments for third-party vendors.

ii. Enhance continuous monitoring and adopt SBOM practices to mitigate supply chain risks.

c. Adoption of Advanced Technologies.

i. Leverage AI and machine learning for threat detection and automated response.

ii. Prepare for post-quantum encryption to future-proof cryptographic defences.

d. Comprehensive Training Programs.

i. Invest in ongoing cybersecurity education for employees to reduce human error and foster a security-conscious culture.

ii. Implement phishing simulation exercises to enhance employee awareness.

e. Regulatory Compliance.

i. Invest in ongoing cybersecurity education for employees to reduce human error and foster a security-conscious culture.

ii. Implement phishing simulation exercises to enhance employee awareness.

f. Zero-Trust Architectures.

i. Strengthen identity verification mechanisms and enforce least-privilege access controls.

ii. Implement micro-segmentation to minimise attack surfaces and lateral movement of threats.

g. Proactive Threat Intelligence.

i. Utilise threat intelligence platforms, such as the Malware Information Sharing Platform (MISP) to anticipate cyber threats.

ii. Implement dark web monitoring to detect potential data breaches and cybercrime activity.

10. By proactively addressing these areas, organisations can strengthen their cybersecurity posture, stay compliant with regulatory requirements, and better navigate the challenges anticipated in 2025.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

. . . . .

REFERENCES

1. Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach

2. Nearly half of employed people have fallen victim to cyberattack or scam. https://nypost.com/2024/09/26/lifestyle/nearly-half-of-employed-people-have-fallen-victim-to-cyberattack-or-scam/

3. Pharmacies across US disrupted following hack at Change Healthcare network. https://www.reuters.com/business/healthcare-pharmaceuticals/change-healthcare-network-hit-by-cybersecurity-attack-2024-02-22/

4. 10 Major Cyberattacks And Data Breaches In 2024 (So Far). https://www.crn.com/news/security/2024/10-major-cyberattacks-and-data-breaches-in-2024-so-far?page=2

5. Top 5 Ransomware Attacks and Data Breaches of 2024. https://www.cybersecurity-insiders.com/top-5-ransomware-attacks-and-data-breaches-of-2024/

6. Company Paid Record-Breaking $75 Million to Ransomware Group: Report. https://www.securityweek.com/company-paid-record-breaking-75-million-to-ransomware-group-report/

7. Report: M&E taking longer to recover from cyber attacks. https://advanced-television.com/2024/11/21/report-me-taking-longer-to-recover-from-cyber-attacks/

8. Insights From Our 2024 CISO Survey Report. https://team8.vc/rethink/enterprise/ciso-survey-2024-report

9. 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/#DBIR2024NR

10. CrowdStrike Update Pushing Windows Machines Into a BSOD Loophttps://cybersecuritynews.com/crowdstrike-update-bsod-loop/

11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

12. SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/newsroom/press-releases/2023-139

13. China Issues New Regulations on Network Data Security Management, Effective January 1, 2025. https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/