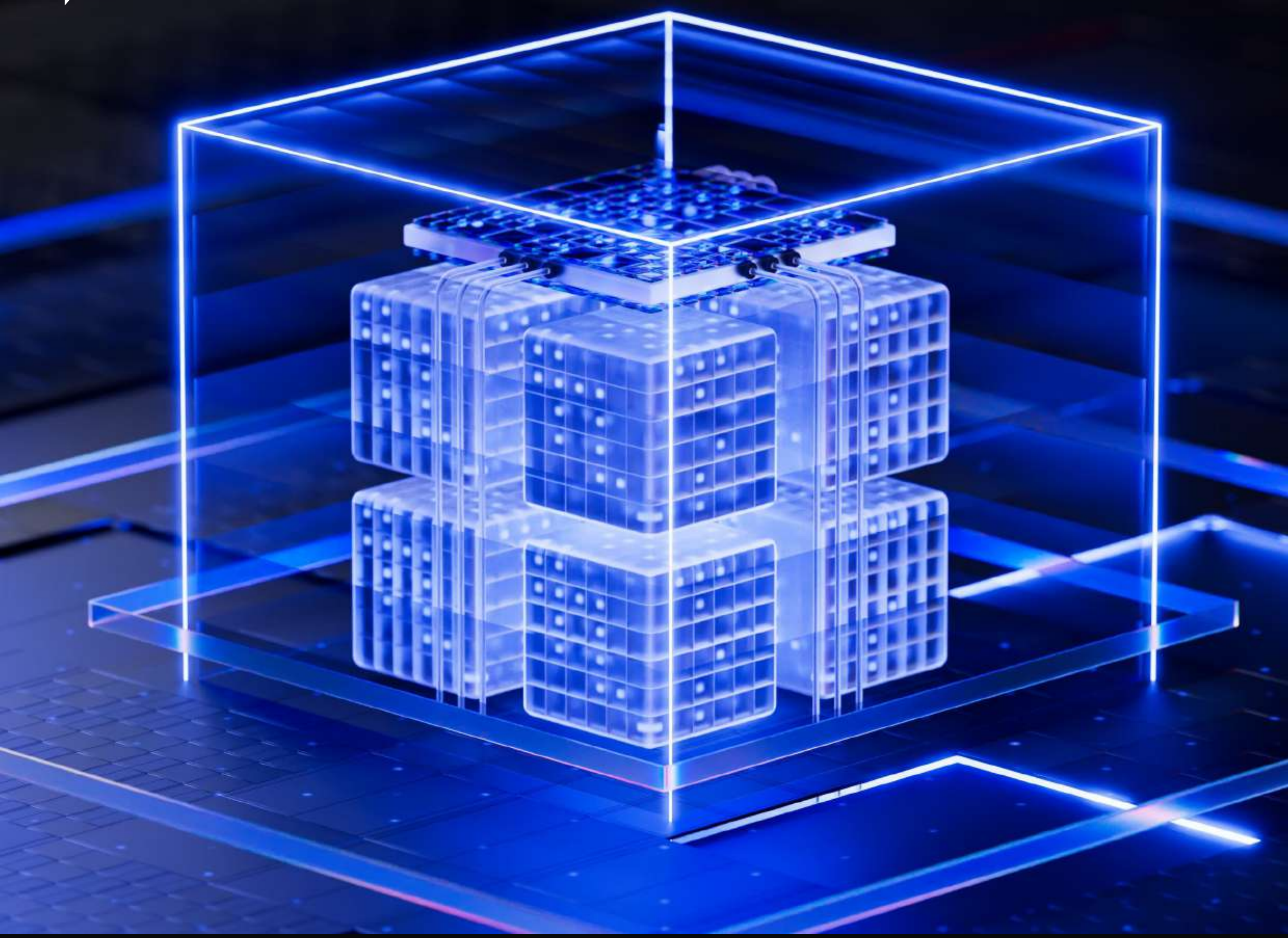
GROUP-IB



SUCCESS STORY

GROUP-IB × HEALTHCARE PROVIDER

How Group-IB ensured uncompromised cybersecurity for one of Malaysia's fastest-growing healthcare provider

About The Healthcare Provider

Country	Malaysia
Industry	Healthcare
Size	**300k+** local and international patients annually **6+** state-of-the-art medical facilities in strategic locations **15+** acclaimed awards in various key competencies, from branding to green initiatives. **90+** resident specialists across **60** areas of specialists.

As one of Malaysia's fastest-growing private healthcare providers, the brand offers extensive specialist services, primary care, and wellness solutions. It is focused on delivering meaningful healthcare experiences to all its patients by providing services built on a passionate commitment to quality, safety, and compassion.

Introduction

The healthcare sector has undergone a massive digital transformation over the past decades. Patient information, medical services, and associated transactional processes are now more accessible and efficient for global patients through websites and applications.

The rapid expansion of data generated online — in both volume and frequency — has made storage, transmission, and analysis easier, but medical information available online needs to be subjected to strict cyber oversight and protection to avoid tampering, leaks, and other cyber threats.

To enable proactive cybersecurity, healthcare providers must continuously assess and monitor risk indicators, alerts, and other signals generated by their entire technology infrastructure to stop threats in real-time. Overlooking security blind spots can significantly weaken an organization's security posture. Such was the case with one of the fastest-growing healthcare providers in Malaysia — who was blinded by the very challenge when a cyber threat escalated into a full-blown attack, prompting them to seek the expertise of a global cybersecurity service provider like Group-IB.

The Malaysian private healthcare provider operates with a high-responsibility mission to save lives, and any delays or disruptions could have catastrophic consequences — an outcome the healthcare provider was determined to avoid. The cyber threat delayed patient care, creating a critical and immediate need to act. Given its high-stakes mission, the provider responded quickly with the help of experts and compensated the threat actor to regain access to sensitive files.

Initial pain points

A ransomware threat from a threat actor previously tracked and researched by Group-IB

Limited context in Threat Intelligence, with no clear indicators of cyber threats, ultimately leaving the healthcare provider vulnerable to ransomware attacks

Subpar risk advisory services

Weak incident response strategy with no Plan of Action (POA) at the time of the attack, leading to delays in Mean Time to Recovery (MTTR) and inadequate support for takedowns

The organization had a traditional and legacy security stack that lacked the necessary capabilities and visibility to defend against modern cyber threats

Lack of visibility into current and emerging vulnerabilities in their network infrastructure, resulting in security gaps

Insufficient critical insights to evaluate and improve the cybersecurity posture

How did Group-IB provide expertise to avert ransomware?

Group-IB Attack Surface Management (ASM)	Group-IB ASM provides businesses with unparalleled visibility into their network activity and infrastructure. It scans for active threats in real-time, prioritizes responses based on risk scoring, and offers automated and expert-guided remediation.
Group-IB Digital Forensics and Incident Response (DFIR)	Group-IB's DFIR experts are ever-ready to block and mitigate attacks quickly to prevent disruption. In the case of ransomware, where every moment counts, our Forensics and Incident Response analysts helped the healthcare provider trace and evidence the attack, and the adversary behind it, which became essential in minimizing damage.
Group-IB Security Assessment	Group-IB assesses every component of your information system to trace, identify, and eliminate potential security gaps that adversaries could exploit.
Group-IB Extended Detection and Response (XDR) and Network Detection and Response (NDR)	Group-IB's XDR and NDR technology performs real-time and historical analysis of attacks through live telemetry and forensic data collection. It also monitors and analyzes network traffic for malicious and suspicious activities, responding to detected cyber threats within the network.

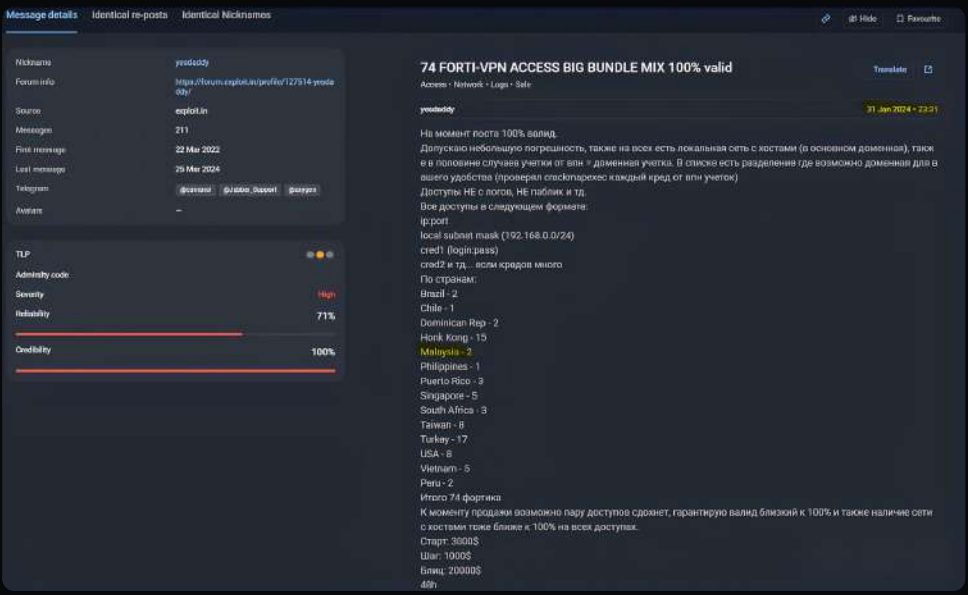
Choice of Cyber Arsenal To Eliminate The Active Threat and Improve Posture

TIn the previous cyber incident, the threat actor's initial access to the healthcare provider's network was via the provider's VPN. At that time, the healthcare provider was using a Fortinet VPN solution. Unfortunately, during that time period, Fortinet Cyber Security Company had a breach that affected a few clients who resided in Malaysia. The consequences of the breach caused Fortinet clients' VPN access/credentials to be sold on the dark web.

The investigation and incident response performed by Group-IB experts concluded that the threat actor had used the VPN credentials purchased from the dark web. The healthcare provider didn't take action when Fortinet was breached because of the absence of threat intelligence advisory and notification.

On January 31, 2024, a threat actor known as “yesdaddy” posted about selling Forti-VPN access to multiple victims, including two Malaysian companies. That same day, a user named “MSSP” initiated an auction for this access pack. By February 2, 2024, another post confirmed that the access was sold through personal messages.

Image source: Post on the dark web made by threat actor for Forti-VPN access



Nickname	yesdaddy
Forum info	https://forum.exploit.in/profile/127514-yesdaddy/
Source	exploit.in
Messages	211
First message	22 Mar 2022
Last message	25 Mar 2024
Telegram	[illegible] @Jabber_Support [illegible]
Avatars	–

TLP	●●●
Admiralty code	
Severity	High
Reliability	71%
Credibility	100%

74 FORTI-VPN ACCESS BIG BUNDLE MIX 100% valid

Access · Network · Logs · Sale

yesdaddy — 31 Jan 2024 • 23:21

На момент поста 100% валид.
Допускаю небольшую погрешность, также на всех есть локальная сеть с хостами (в основном доменная), также в половине случаев учетки от впн = доменная учетка. В списке есть разделение где возможно доменная для вашего удобства (проверял crackmapexec каждый кред от впн учеток)
Доступы НЕ с логов, НЕ паблик и тд.
Все доступы в следующем формате:
ip:port
local subnet mask (192.168.0.0/24)
cred1 (login:pass)
cred2 и тд... если кредов много.
По странам:
Brazil - 2
Chile - 1
Dominican Rep - 2
Honk Kong - 15
Malaysia - 2
Philippines - 1
Puerto Rico - 3
Singapore - 5
South Africa - 3
Taiwan - 8
Turkey - 17
USA - 8
Vietnam - 5
Peru - 2
Итого 74 фортика
К моменту продажи возможно пару доступов сдохнет, гарантирую валид близкий к 100% и также наличие сети с хостами тоже ближе к 100% на всех доступах.
Старт: 3000$
Шаг: 1000$
Блиц: 20000$
48h

Given the timing, Malaysian context, and the Forti-VPN access, the Group-IB Threat Intelligence team suspected the healthcare provider’s VPN access was likely sold on the dark web.

Immediate steps for threat response and interdiction were taken to deal with the active ransomware, along with other technology activations such as:

Attack Surface Management

- ✓ Group-IB Attack Surface Monitoring (ASM) was deployed so that the solution can notify the customer whenever a **leaked credential** is associated with the assets being monitored. With the help of Group-IB Threat Intelligence (TI), ASM informs the customer in real-time about targeted data breaches and publicly available data breaches. Through this capability, we **learned what caused the initial access from the threat actor.**
- ✓ **Dark web mention** — With TI data, Attack Surface Management identifies whether adversaries have mentioned any of the customer's assets on the dark web and offers high-level access to underground platforms for review and threat mitigation.

Learn more about it

Security Assessment

- ✓ The collaboration between Group-IB and the healthcare brand began with assessing the complete scope of the damage. Experts conducted a comprehensive security assessment to locate and manage risks effectively across IT systems.
- ✓ We identified unknown vulnerabilities and implemented high-impact changes through tailored guidelines and strategies.

Learn more about it

Incident Response to Ransomware

- ✓ Group-IB helped the healthcare provider negotiate the terms with the ransomware group. Our experts assisted them in decrypting the ransomware-encrypted data and restoring critical systems and data. This rapid recovery minimized the incident's impact on their business operations and prevented further financial losses.
- ✓ This dual approach allowed the healthcare provider to address the technical and operational aspects of the incident simultaneously.

Learn more about it

Digital Forensics

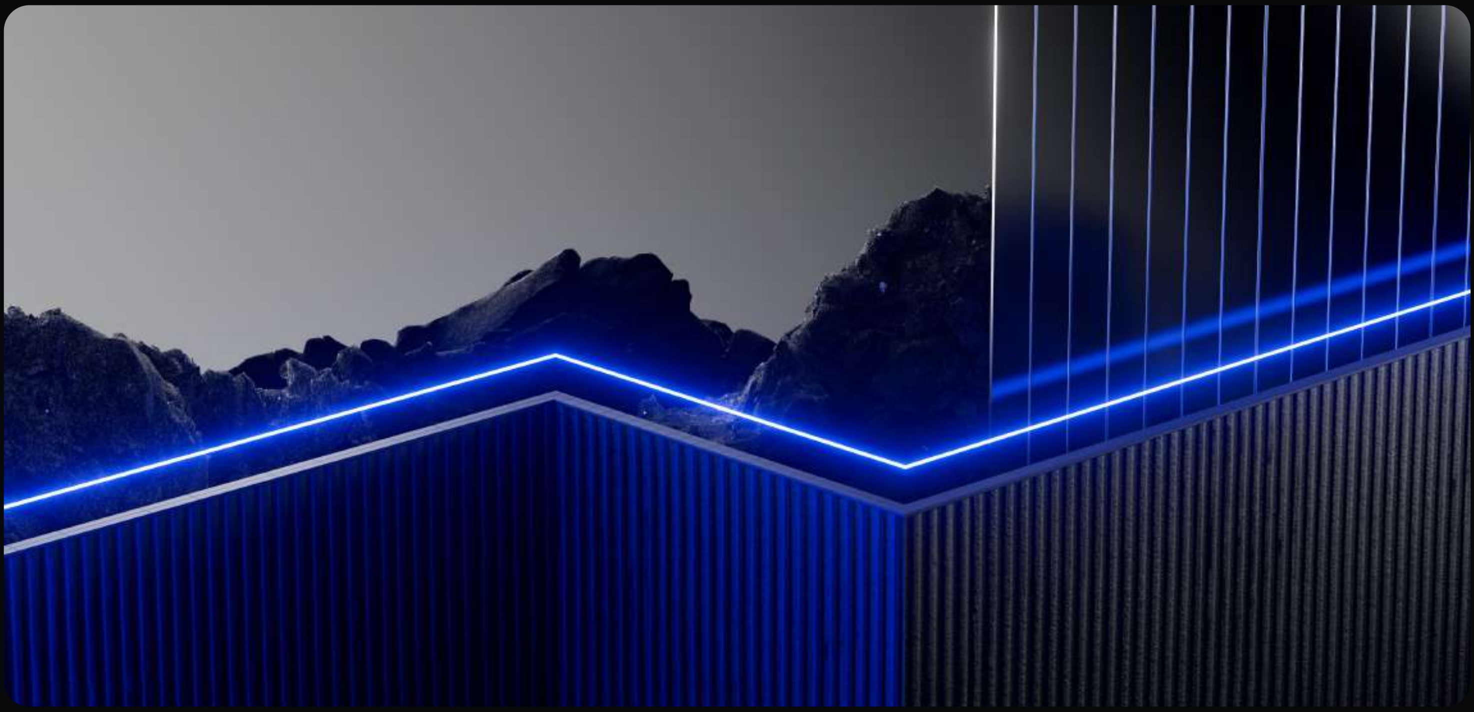
- ✓ Group-IB's digital forensics team conducted a thorough investigation to trace the attack's origin, exploited vulnerabilities, and the methods used by the threat actor. The root cause was a Fortigate Firewall, which also provides SSL VPN services for the healthcare provider's staff to connect to the internal network from external locations.
- ✓ Group-IB helped reveal the full scope of the breach, assess the extent of the damage, and collect critical evidence.

Learn more about it

Network Detection & Response (NDR) and Extended Detection & Response (XDR)

Learn more about it

- ✓ XDR and NDR solutions enabled advanced threat hunting, detection, and response.
- ✓ Group-IB's solutions provided comprehensive protection across email, network, and endpoints, effectively blocking many previously unnoticed or hidden threats.
- ✓ Post-incident support with XDR tools and threat-hunting services ensured no further risks or disruptions occurred in the healthcare provider's network.



"Group-IB stood out due to their deep expertise in threat intelligence, incident response, and cybercrime investigations. Their proven track record in handling complex and sophisticated cyberattacks and innovative solutions like Extended Detection & Response (XDR) and Network Detection & Response (NDR) aligned with our security objectives. Unlike other providers, Group-IB offered a comprehensive approach and a clear path to enhancing our security posture."

Quote by the Healthcare Provider

Results?

Retaliation against Ransomware

- ✓ Successful resolution and recovery of encrypted data.
- ✓ Blocked 2,872 malicious threats during March and April 2024

Defenses against threats

- ✓ Backdoor Malware
- ✓ Remote Access Trojans (RAT)
- ✓ Ransomware KillSwitch
- ✓ EternalBlue
- ✓ Cryptojacking
- ✓ Adware
- ✓ Trojans
- ✓ Stealer Malware

Minimizing Damage

- ✓ Extended expertise in recovering encrypted assets and restoring critical systems and data.
- ✓ Prevention of further operational and financial losses.

Security enhancements

- ✓ Streamlined security processes and improved overall security posture with Group-IB solutions.
- ✓ Automated threat detection and response led to better risk management and IT resource allocation, shifting from reactive to proactive cybersecurity with Group-IB's expert guidance.

2872

malicious threats was blocked during March and April 2024

Conclusion

This collaboration study highlights a strong partnership that enabled a strategic response to the ransomware attack followed by a comprehensive network audit and gap analysis, strengthening cybersecurity for the private healthcare provider. Group-IB's industry-leading team, with over 1,550+ global investigations and 70,000 hours of incident response experience, leveraged patented technologies and investigative expertise to swiftly resolve the crisis, identify potential vulnerabilities and ensure capabilities were in place to address any emerging risks in the infrastructure immediately.

These strengths made Group-IB the top choice for Malaysia's rapidly growing healthcare provider, with the team citing Group-IB's solutions, expertise, experience, proven track record in cybersecurity, and unique knowledge about the particular threat actor as the primary reasons.

Unprecedented challenges require expert cybersecurity guidance

If you suspect or are experiencing a ransomware attack, contact us through Group-IB's immediate helpline: response@cert-gib.com. To build an end-to-end protection strategy against ransomware and other advanced threats,

Visit our dedicated page or Give our experts a nudge here

About Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,550+ Successful investigations of high-tech cybercrime cases	**400+** employees	**600+** enterprise customers	**60** countries
$1 bln saved by our client companies through our technologies	**#1*** Incident Response Retainer vendor	**120+** patents and applications	**8** Unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL

EUROPOL

AFRIPOL

Recognized by top industry experts

FORRESTER

Aite Novarica

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785