ISSUE 1

JAN-JUN 2025

CyberSec Savvy

CYBER ATTACKS IN THE PACIFIC ISLANDS

JAN-JUN 2025

THREAT INTELLIGENCE BRIEF

JANUARY 2025

PAPUA NEW GUINEA

The **Inland Revenue Commission (IRC)** suffered a ransomware attack on January 28, 2025.

- Systems affected: tax processing (SIGTAS), emails, phones
- Suspected group: **Ransomhub**
- PNG declined to pay ransom; KPMG led forensics

What You Need To Know About RANSOMHUB

Type: Ransomware-as-a-Service (RaaS)

Active Since: 2024

Tactics and Techniques:

- Affiliates and manage their own wallets (10% cut to the core group)
- Written in GoLang; uses Gobfuscate for obfuscation
- Initial access via phishing, password spraying, and CVE exploitation

Tools: Mimikatz, AngryIPScanner, PowerShell, Rclone

Exploits: Citrix ADC, FortiOS, Confluence, SMBv1, Netlogon

Notable Insight: Ransomhub was the most prolific ransomware group in early 2025, but its infrastructure collapsed in March, with some affiliates migrating to Qilin.

REGIONAL INSIGHT

Samoa's CERT issued its first APT40 advisory, warning of Chinese state-linked cyber espionage targeting Pacific government networks.

FEBRUARY 2025

PALAU

The **Ministry of Health & Human Services (Belau National Hospital)** was hit by **Qilin ransomware** on February 20, 2025.

- Systems at the Belau National Hospital were compromised
- Patient data from 2018-2022 was exposed
- U.S. Cyber Command assisted with recovery

What You Need To Know About QILIN

Type: Ransomware-as-a-Service (RaaS)

Active Since: 2022 (formerly “Agenda”)

Tactics & Techniques:

- Double extortion: encrypts + leaks data
- Written in Rust for cross-platform attacks
- Uses Safe Mode execution, backup deletion, and log wiping
- Targets high-value sectors: healthcare, retail, telecom
- Affiliates often gain access via phishing or exploiting VPNs and Veeam vulnerabilities

NOTABLE INSIGHT: Qilin surged in 2025, filling the vacuum left by collapsing groups like Ransomhub. It became the dominant ransomware group globally by mid-year.

REGIONAL INSIGHT

- Samoa’s public attribution of APT40 marked a turning point in Pacific cyber diplomacy.
- Samoa and PNG highlighted in ASPI’s analysis as examples of the urgent need for cyber resilience and capacity building.
- Increased calls for regional CERT collaboration and foreign technical assistance, especially from Australia, Japan, and the U.S.

MARCH 2025

What You Need To Know About ARCUSMEDIA

Type: Ransomware-as-a-Service (RaaS)

Active Since: May 2024

Tactics & Techniques:

- Double extortion with ChaCha20 + RSA-2048 encryption
- Delete shadow copies, clears logs, disables recovery
- Uses ShellExecuteExW for privilege escalation
- Targets: government, retail, media
- Persistence via registry autostart entries

NOTABLE INSIGHT: ArcusMedia is known for anti-forensics and stealth. It's a rising player in the ransomware ecosystem, often using TOR-based C2 channels.

KIRIBATI

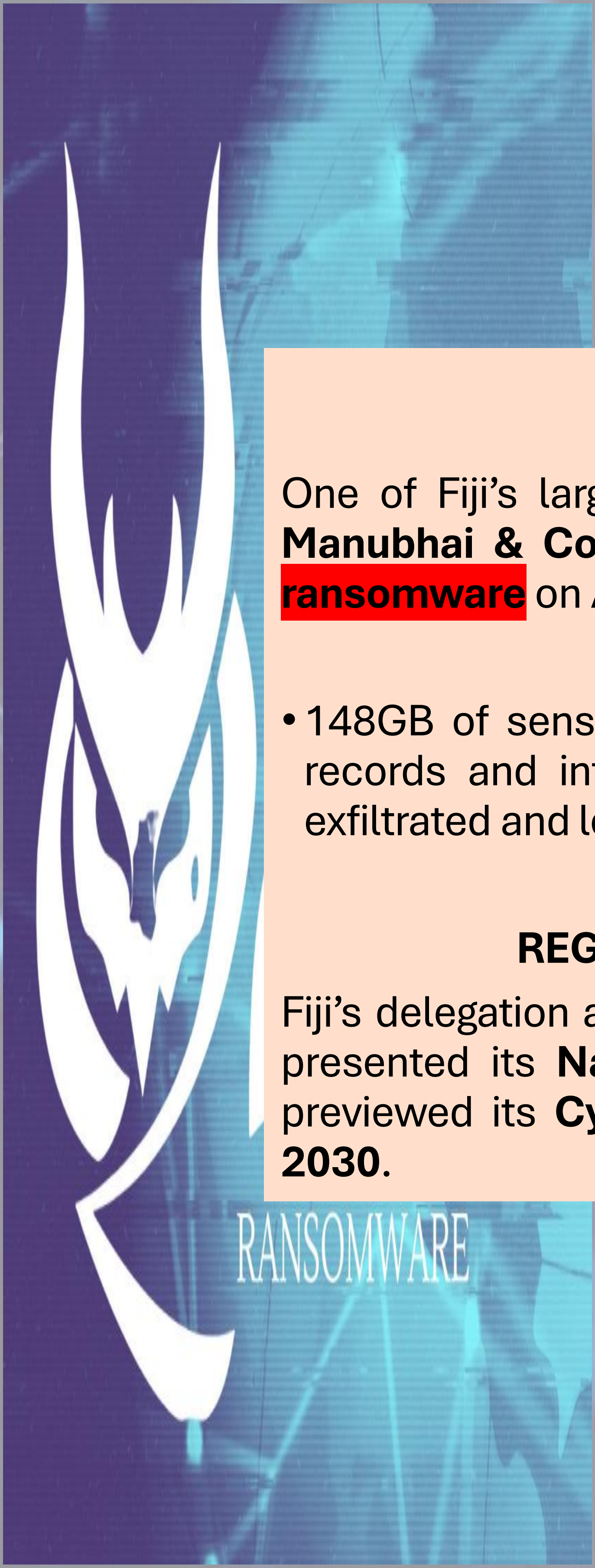
The government domain **kao.gov.fj** was compromised by **ArcusMedia ransomware** on March 18, 2025.

- Encrypted critical systems and surfaced on dark web leak sites.
- Limited public disclosure; likely involved data exfiltration.

REGIONAL INSIGHT

- Tonga and Kiribati were flagged in a regional CERT report as lacking disaster recovery infrastructure and cyber incident response playbooks.
- Vanuatu began consultations on forming a National Cybersecurity Taskforce.

APRIL 2025



FIJI

One of Fiji’s largest hardware suppliers**, RC Manubhai & Co. PTE LTD**, was hit by **Qilin ransomware** on April 28, 2025.

- 148GB of sensitive data, including financial records and internal communications, was exfiltrated and leaked.

REGIONAL INSIGHT

Fiji’s delegation at the **RSA Conference 2025** presented its **National Digital Strategy** and previewed its **Cybersecurity Strategy 2025-2030**.

MAY 2025

No confirmed cyber attacks reported in Pacific Islands nations during May 2025.

However, regional CERTs issued alerts about:

- Surge in phishing and infostealer campaigns, especially targeting government email systems.
- CERTs warned of credential harvesting.

What You Need To Know About INFOSTEALER MALWARE

Type: Malware-as-a-Service (MaaS)

Tactics & Techniques:

- Delivered via phishing, fake software, cracked apps.
- Steals browser credentials, cookies, crypto wallets.
- Logs sold on dark web or used for BEC and ransomware.
- Common variants: LummaC2, StealC, Atomic Stealer (AMOS).

NOTABLE INSIGHTS: INTERPOL's Operation Secure (Jan-Apr 2025) dismantled over 20,000 malicious IPs and domains linked to infostealers across Asia-Pacific, including Fiji, Samoa, and PNG.

REGIONAL INSIGHT

The activation of Fiji CERT and the development of the Cybersecurity Strategy 2025-2030 were publicly highlighted.

JUNE 2025

TONGA

The **National Health Information System (NHIS)** was taken offline by **Inc Ransomware** on June 26, 2025.

- The entire health system was taken offline.
- Ransom demand: USD $1 million.
- Manual recordkeeping resumed.
- No backup offsite and disaster recovery site in place.

What You Need To Know About Inc Ransom (IncRansom)

Type: Ransomware-as-a-Service (RaaS)

Active Since: 2023

Tactics & Techniques:

- Double extortion with TOR-based ransom portal
- Uses Rclone, AnyDesk, and Impacket for lateral movement.
- Deletes backups and prints ransom notes via network printers.
- Often targets healthcare and government agencies.

NOTABLE INSIGHTS: CERT Tonga issued a region-wide advisory in June 2025, warning of IncRansom's growing presence in the Pacific. The group is known to handle extortion and payments directly, not just via affiliates.

FIJI

One of Fiji's largest Retail Conglomerates, **Tappoo Group of Companies**, was breached by **Qilin ransomware** on June 26, 2025.

REGIONAL INSIGHT

- Fiji and JICA signed a landmark MoU to support cybersecurity capacity building across 14 Pacific nations.
- Movement towards regional cyber diplomacy, with Japan, the U.S., and Australia supporting Pacific-led resilience initiatives.

REGIONAL TRENDS (JAN – JUN 2025)

- **Double Extortion**: Encrypt + steal + leak threats
- **Healthcare & Government**: Most targeted sectors
- **No Ransom Paid**: All governments refused to pay
- **Manual Recovery**: Tonga and PNG reverted to offline operations.
- **CERT Gap**s: Kiribati and Tonga lack fully staffed CERTs

WHAT CAN BE DONE?

- Establish a Pacific Cybersecurity Alliance
- Fund and train regional CERTs
- Mandate off-site backups and incident response plans
- Conduct tabletop ransomware simulations

FINAL WORD

From tax systems to hospitals and retail giants, ransomware groups are no longer ignoring the Pacific Islands.

They are embedding it into their playbooks.

The first half of 2025 has made one thing clear:

“The Pacific is no longer off the grid.”