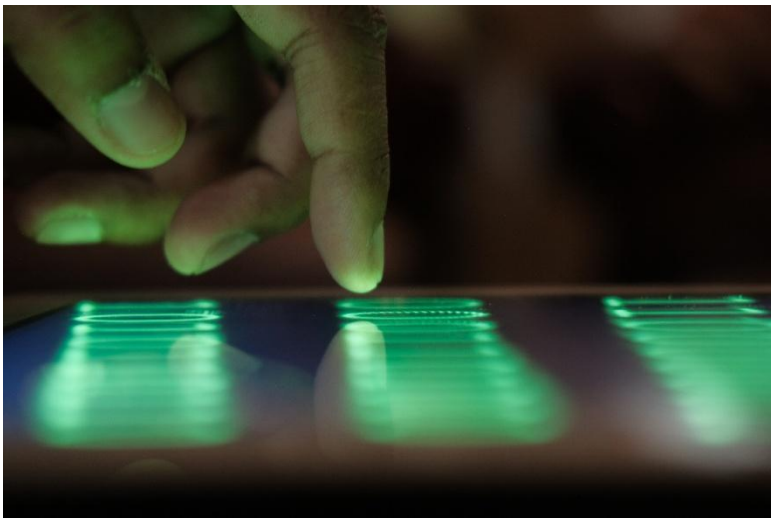

A Review of Cyber Threats Targeting Fiji

TRENDS, THREAT ACTORS, AND STRATEGIC IMPLICATIONS

Harry Robinson | Extremelynonlinear.com | 2025

Contents

1.Executive Summary

This report provides a cyber threat intelligence (CTI) assessment of the Fijian Government's evolving cybersecurity landscape. It focuses on the strategic implications of the 2021 ransomware attack by the Sodinokibi (REvil) group, examines Fiji's regional cyber posture, and offers actionable recommendations to improve national cyber resilience.

While Fiji has made commendable strides in developing cyber capabilities—including its membership in PaCSON, the formation of a Cyber Crime Unit, and the planned operationalization of a national CERT—the country remains an attractive target for financially motivated cybercriminals. The *REvil* incident revealed critical vulnerabilities in government infrastructure but also demonstrated resilience through a prompt recovery and refusal to meet ransom demands.

In parallel, the Pacific Islands region is facing increasing geopolitical competition, with Australia and China both vying for strategic influence through investments and partnerships. With the cyber domain now being recognized as a strategic competition point, the importance of a robust, coordinated cybersecurity posture for Fiji and its neighbours is further elevated.

The report also explores the growing threat of cybercrime targeting Fijian citizens, particularly through scams and financial fraud. It concludes with a set of strategic, operational, and community-level recommendations aimed at strengthening Fiji's cyber readiness, protecting its digital economy, and reinforcing public trust in government services.

2.Introduction and Scope

Fiji, a developing island nation with a population of just over 900,000, is undergoing rapid digital transformation amid a complex regional security environment. Despite advancements in connectivity and e-governance, Fiji's cyber infrastructure and policy frameworks remain less mature than those of its regional counterparts, Australia and New Zealand.

Recent years have brought increased cyber threats to the Pacific, including ransomware attacks, espionage campaigns, and a surge in online scams targeting individuals. These incidents have underscored the urgent need for enhanced cybersecurity readiness and regional cooperation. Fiji's membership in the Pacific Cyber Security Operational Network (PaCSON) and its collaboration with the Australian Cyber Security Centre (ACSC) represent important steps toward building resilience.

This report focuses on the 2021 cyberattack attributed to the *REvil* (*Sodinokibi*) ransomware group and uses this incident as a case study to examine broader strategic

implications for Fiji. It applies the MITRE ATT&CK framework to map likely tactics, techniques, and procedures (TTPs), compare analogous case studies, and assesses the evolving threat landscape—including state-sponsored intrusions and financially motivated scams.

The goal of this report is to provide insight into how Fiji can strengthen its cybersecurity posture in light of ongoing threats, regional dynamics, and emerging trends.

3.Regional Context

Fiji is a developing Pacific Island nation with a population of just over 900,000. As such, its digital environment, cyber infrastructure, expertise, and policies have yet to reach the maturity levels of its regional neighbours, Australia and New Zealand.

3.1 Cyber Readiness

Fiji is a member of the Pacific Cyber Security Operational Network (PaCSON). According to their website, they are a working-level network of cybersecurity and technical experts from eligible Pacific governments. PaCSON is supported by the Australian Cyber Security Centre (ACSC) (PaCSON, n.d.).

The Fiji Police Force has established a dedicated Cyber Crime Unit, and the government has begun plans to operate a National Computer Emergency Response Team (CERT) under the Department of Communications (Chand, 2025) (FIJI STRENGTHENS CYBERSECURITY WITH ESTABLISHMENT OF FIJI CERT AND NATIONAL STRATEGY, 2024).

Additionally, the Australian Government has invested over $26 million to establish Cyber Rapid Assistance for Pacific Incidents and Disasters (Cyber RAPID) teams, led by the Department of Foreign Affairs (Cyber Affairs and Critical Technology, n.d.).

3.2 Regional Geopolitical Dynamics

As a former British colony, Fiji has traditionally aligned with the region's major power players—Australia and New Zealand. Suva, Fiji's capital, is home to the main campus of the Pacific's largest university, the University of the South Pacific (USP). The university has benefited from a long-standing partnership with Australia, which has provided core funding, infrastructure support, and project-based assistance. Australia has also supported key strategic plans and initiatives across education, climate resilience, research, and digital connectivity. This collaboration has delivered tangible benefits for both the university and the broader Pacific region (Development Partners/Donor Profiles, 2025).

In 2022, the Australian Government further demonstrated its commitment to the region by completing construction of a $100 million military training facility in Fiji, aimed at

enhancing the country's capacity for peacekeeping, humanitarian assistance, and disaster relief (Sajid, 2022).

However, China's influence in Fiji—and the wider Pacific—continues to grow. A policing cooperation agreement between Fiji and China, which initially raised concerns in Australia, was briefly suspended in 2022 by the incumbent Prime Minister but has since been reinstated (Fiji upholds China policing agreement, Guardian Australia reports, 2024). Additionally, a Confucius Institute has operated from the University of the South Pacific for over a decade, further highlighting China's soft power presence in the region (Confucius Institute provides platform between China, Fiji, 2017).

Additionally, in 2013, China launched the Belt and Road Initiative (BRI), a global infrastructure development strategy aimed at reviving and expanding the ancient Silk Road. The initiative seeks to create a vast network of Chinese-funded infrastructure projects that would connect Lisbon, Portugal, to the heart of the South Pacific. (James McBride, 2023)

Analysts have long speculated that the Pacific region holds strategic appeal for China, particularly due to its potential as a site for future military bases and influence projection. (Brady, 2022)

3.3 Legal/policy Frameworks

Fiji enacted the Cybercrime Act 2021, which aligns with the Budapest Convention on Cybercrime (Pratap, 2023). However, the nation has yet to finalize its new National Cyber Strategy (Kumar, 2025).

4.Threat Landscape Overview

4.1 Attacks

In 2024, the Pacific Islands Forum (PIF) Secretariat was the target of a significant cyberattack. The intrusion appeared to be aimed at gathering intelligence on the Secretariat's internal operations. In response, The Australian Government deployed one of its roving teams of cyber RAPID specialists—comprised of both government and private sector experts—to Fiji to assist the Secretariat in responding to the incident. An incident report is yet to be publicly released, however analysis by the Australian Cyber Security Centre found that the attack can be attributed to a group backed by the Chinese government (Dziedzic, n.d.).

In 2021, the Fijian Government's Information Technology and Computing Services (ITC) Department experienced a significant cyber incident when the Russia-based ransomware group *Sodinokibi* (*REvil*) infiltrated the government's network. The attackers exfiltrated sensitive data and posted screenshots on their leak site, demanding payment to prevent

further disclosure. The breach disrupted online services, including the COVID-19 vaccination registration portal, prompting a temporary shutdown of government networks to safeguard system integrity (Cyber Incident Victim: Fiji Government, 2021).

4.2 Cybercrime

Finally, cybercrime and scams are an increasingly common occurrence in Fiji. In 2023, the notorious *EbayShop* Online Recruitment pyramid scheme defrauded thousands of Fijians, resulting in financial losses exceeding $3 million and prompting over 1,700 complaints to authorities (EBayShop Online Recruitment scam, 2023). Additionally, the Criminal Investigations Department is investigating 650 *M-PAiSA* scam cases, with reported losses totaling more than $614,000 (Vucukula, 2024) . These incidents highlight the growing prevalence of online financial fraud in the country.

The 2024 State of Scams in Fiji report, conducted by the Global Anti-Scam Alliance (GASA), reveals that over half of Fijians encounter scams at least monthly, with shopping, investment, and identity theft scams being the most prevalent. Despite 66% of respondents expressing confidence in identifying scams, underreporting remains a significant issue, primarily due to skepticism about the effectiveness of reporting mechanisms and uncertainty about where to report. Scammers predominantly use instant messaging apps and social media platforms, such as Facebook and Gmail, to perpetrate fraud, often causing substantial emotional and financial distress to victims. The report underscores the need for enhanced public awareness, improved reporting processes, and stronger protective measures to combat the growing threat of scams in Fiji. (FCCC, 2024)

5.REvil Threat Actor Analysis

As mentioned in 4.1, the Russia-based ransomware group *Sodinokibi (REvil)* was thought to be behind the 2021 attack on the Fijian Government's Information Technology and Computing Services (ITC) Department.

5.1. MITRE ATT&CK-Informed TTP Mapping

As we don't have detailed technical evidence from this attack, we can reasonably infer REvil's behavior by examining their globally observed TTPs (MITRE, 2024). In line with the MITRE ATT&CK framework, here's how they typically operate — and here's how that likely applied in the Fijian Government context:

TA0043 – Reconnaissance

T1595 – Active Scanning: REvil affiliates may have conducted active scanning to identify vulnerable systems within the Fijian Government's network.

T1592 – Gather Victim Host Information: Information about host configurations and software versions could have been collected to tailor the attack strategy.

TA0042 – Resource Development

T1583.006 – Acquire Infrastructure: Web Services: REvil operators often set up malicious web services to host payloads or command-and-control (C2) infrastructure.

T1584.001 – Compromise Infrastructure: Domains: They may have compromised legitimate domains to use in phishing campaigns or to distribute malware.

TA0001 – Initial Access

T1190 – Exploit Public-Facing Application: REvil has exploited vulnerabilities in public-facing applications, such as Oracle WebLogic Server, to gain initial access.

T1189 – Drive-by Compromise: Users visiting compromised websites could have inadvertently downloaded and executed REvil payloads.

TA0002 – Execution

T1059.001 – Command and Scripting Interpreter: PowerShell: REvil utilizes PowerShell scripts to execute malicious commands and deploy ransomware.

T1059.003 – Command and Scripting Interpreter: Windows Command Shell: The group employs command-line interfaces for executing various tasks, including disabling security features.

TA0003 – Persistence

T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder: REvil may establish persistence by adding entries to the registry or startup folders.

T1053.005 – Scheduled Task/Job: Scheduled Task: Creating scheduled tasks to maintain access and execute payloads at specified times.

TA0004 – Privilege Escalation

T1134.001 – Access Token Manipulation: Token Impersonation/Theft: REvil can impersonate tokens to escalate privileges within the system.

T1068 – Exploitation for Privilege Escalation: Exploiting vulnerabilities to gain higher-level permissions on compromised systems.

TA0005 – Defense Evasion

T1140 – Deobfuscate/Decode Files or Information: REvil decodes or deobfuscates its payloads at runtime to hinder static analysis.

T1027 – Obfuscated Files or Information: The group uses obfuscation techniques to conceal malicious code.

TA0006 – Credential Access

T1003.001 – OS Credential Dumping: LSASS Memory: REvil extracts credentials from the Local Security Authority Subsystem Service (LSASS) memory.

T1555.003 – Credentials from Password Stores: Credentials from Web Browsers: Harvesting credentials stored in web browsers.

TA0007 – Discovery

T1083 – File and Directory Discovery: Scanning the file system to identify files for encryption.

T1087.001 – Account Discovery: Local Account: Enumerating local user accounts to facilitate lateral movement.

TA0008 – Lateral Movement

T1021.002 – Remote Services: SMB/Windows Admin Shares: REvil propagates through shared network resources.

T1076 – Remote Desktop Protocol: Utilizing RDP to move laterally across the network.

TA0009 – Collection

T1119 – Automated Collection: Automatically collecting files and information from compromised systems.

T1005 – Data from Local System: Gathering data stored on local systems for exfiltration.

TA0011 – Command and Control

T1071.001 – Application Layer Protocol: Web Protocols: Using HTTP/HTTPS for command-and-control communications.

T1573.002 – Encrypted Channel: Asymmetric Cryptography: Establishing encrypted channels to evade detection.

TA0010 – Exfiltration

T1041 – Exfiltration Over C2 Channel: Transferring collected data over established command and control channels.

T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage: Uploading data to cloud storage services for exfiltration.

TA0040 – Impact

T1486 – Data Encrypted for Impact: Encrypting data on infected systems to demand ransom payments.

T1490 – Inhibit System Recovery: Deleting shadow copies and disabling recovery features to prevent data restoration.

These inferred behaviors align with REvil's known operational patterns and provide a framework for understanding the potential tactics employed during the attack on the Fijian Government's ITC Department.

6.Analogous Case Studies

MITRE ATT&CK Framework Mapping

In April 2021, the Italian pharmaceutical company Mipharm SPA was targeted by the Sodinokibi (REvil) ransomware group. The attack involved data exfiltration and public exposure of confidential information, aligning with REvil's known tactics.

Based on the MITRE ATT&CK framework, the following techniques were likely employed:

TA0001 – Initial Access

T1190 – Exploit Public-Facing Application: REvil has exploited vulnerabilities in applications like Oracle WebLogic Server to gain initial access.

TA0002 – Execution

T1059.001 – Command and Scripting Interpreter: PowerShell: Utilization of PowerShell scripts to execute malicious commands.

TA0005 – Defense Evasion

T1027 – Obfuscated Files or Information: Employing obfuscation techniques to conceal malicious code.

TA0010 – Exfiltration

T1041 – Exfiltration Over C2 Channel: Transferring collected data over established command and control channels.

TA0040 – Impact

T1486 – Data Encrypted for Impact: Encrypting data on infected systems to demand ransom payments.

6.1 Indicators of Compromise (IOCs)

While specific IOCs for the Mipharm SPA incident was not publicly disclosed, REvil's operations have been associated with various IOCs in other incidents. For example, during the Kaseya VSA attack, the following IP addresses were observed:

18.223.199.234, 35.226.94.113, 161.35.239.148, 162.253.124.162 (Gil, 2021)

Additionally, REvil samples have been identified with specific file hashes, such as:

SHA256: 861bc212241bcac9f8095c8de1b180b398057cbb2d37c92220086ffaf24ba9e08

(Team, 2019)

6.2 Application in Fiji's Context

Given the similarities in attack patterns, the Fijian Government's ITC Department could consider the following measures:

Network Monitoring: Implement monitoring for known malicious IP addresses associated with REvil to detect potential intrusions.

File Integrity Checks: Regularly verify file hashes against known malicious samples to identify unauthorized changes.

Employee Training: Educate staff on phishing tactics and the importance of not interacting with suspicious emails or links.

Incident Response Planning: Develop and regularly update incident response plans to quickly address potential ransomware attacks.

By analyzing the Mipharm SPA incident, Fiji can enhance its cybersecurity posture against similar threats posed by groups like REvil.

7.Impact Assessment

While technical specifics were not disclosed publicly, based on REvil's known modus operandi, the impact on Fiji's critical services and public trust could be extrapolated as follows:

7.1 Internal Government Stability

The immediate fallout of *REvil's* attack was the disruption of critical government COVID-19 services, unauthorized access to government servers and data leaks (Turaga, 2021). It is reasonable to expect that citizen trust in digital government services may have been impacted as a result of the attack, particularly in the absence of transparent communication or rapid recovery.

Strategically, one potential consequence could be that Cybersecurity incidents of this nature can lead to institutional caution around future digital transformation efforts — especially in environments where cyber maturity or response frameworks are still developing. Leaders may become risk-averse, delaying or deprioritizing initiatives that involve expanded data handling or public-facing infrastructure.

7.2 External Perception and Diplomacy

It is reasonable to assess that the *REvil* attack had minimal long-term impact on Fiji's international cyber reputation. As a developing nation with limited cyber infrastructure and political volatility, Fiji is often perceived as a low-hanging target for opportunistic actors. In such contexts, a delayed or disrupted response may be expected. However, the Fijian Government's refusal to pay a ransom, coupled with its restoration of services within a week, positioned the incident less as a reputational failure and more as a demonstration of operational resilience. In this sense, the event could be interpreted as a form of readiness test — one in which Fiji performed credibly.

There is little doubt that this attack served as a catalyst — either for initiating cyber reform and greater Cyber readiness, or for accelerating its urgency.

8.Future Outlook

Financial gain remains the primary motivator for cyberattacks against Fiji. Looking ahead, public scans still show some exposed services in the Fijian Government IP space. This continued exposure presents opportunities for ransomware groups to repeat or escalate attacks. While the *REvil* attack may have succeeded in disrupting Fijian government services, intelligence reporting indicates that the Sodinokibi (*REvil*) group primarily operates with financial motivation. Given that no ransom was paid, the operation could be considered unsuccessful from the attackers' perspective. As such, Fiji's refusal to engage with the ransom demand — and its ability to restore services — may serve as a signal to other threat actors that the nation maintains a degree of cyber resilience, particularly with support from regional partners such as the Australian Cyber Security Centre.

As Fiji continues to strengthen its government-level cyber resilience, financially motivated threat actors may increasingly pivot toward targeting individuals through online scams. The general public remains particularly vulnerable, as evidenced by incidents such as the *eBay Shop* online recruitment pyramid scheme and the 650 reported *M-PAiSA* scam cases.

9.Recommendations

91. Strategic

Finalize and Implement a National Cyber Strategy: Accelerate the release and adoption of Fiji's upcoming cyber strategy to provide a coordinated framework for protecting critical systems and improving national cyber resilience.

Formally Operationalize Fiji CERT: Ensure the Computer Emergency Response Team (CERT) is fully funded, staffed, and empowered to act as a national focal point for incident response, threat intelligence sharing, and public education.

Develop a Centralized National Incident Response Plan: This should include clear procedures for cross-agency collaboration, coordination with regional partners like ACSC, and public communication during cyber events.

Enhance Regional Partnerships: Continue leveraging support from Australia (e.g., ACSC, Cyber RAPID) and strengthen involvement in PaCSON to access shared intelligence, response capabilities, and training opportunities.

92. Operational

Conduct Regular External Exposure Assessments: Use tools like Shodan or partner services to routinely scan government IP ranges for vulnerable or misconfigured services and implement patching or access restrictions as needed.

Establish a National Threat Intelligence Feed: Integrate regional threat intelligence with IOCs from known actors like REvil to proactively detect and mitigate risks across government networks.

Mandate Cybersecurity Audits for Critical Government Services: Especially those related to healthcare, law enforcement, and citizen services. This can help detect insecure legacy systems and reinforce cyber hygiene.

9.3 Community

Launch a National Cyber Awareness Campaign: Collaborate with telecom providers, banks, and social platforms to improve scam literacy and phishing awareness among citizens, especially vulnerable populations.

Introduce a Central Scam Reporting Platform: This should be simple, accessible, and well-publicized — reducing underreporting and enabling quicker disruption of scam networks.

Incorporate Cybersecurity Education in Schools and Public Training Programs: Building digital resilience from the ground up will reduce Fiji's long-term vulnerability to both nation-state threats and financially motivated cybercrime.

10. Bibliography

(n.d.). Retrieved from PaCSON: https://pacson.org/

(n.d.). Retrieved from https://en.wikipedia.org/wiki/Belt_and_Road_Initiative

(2024). Retrieved from FCCC: https://fccc.gov.fj/wp-content/uploads/2025/03/State-of-Scams-Report-Fiji-2024.pdf

Brady, A.-M. (2022). *China in the Pacific: from 'friendship' to strategically placed ports and airfields*. Retrieved from ASPI: https://www.aspistrategist.org.au/china-in-the-pacific-from-friendship-to-strategically-placed-ports-and-airfields/

Chand, A. (2025, March 23). *Bolstering cyber crime unit in police reset plan*. Retrieved from The Fiji Times: https://www.fijitimes.com.fj/bolstering-cyber-crime-unit-in-police-reset-plan/

Confucius Institute provides platform between China, Fiji. (2017). Retrieved from http://en.people.cn/n3/2017/1014/c90000-9279731.html

Cyber Affairs and Critical Technology. (n.d.). Retrieved from Depertment of Foreign Affairs and Trade: https://www.dfat.gov.au/international-relations/themes/cyber-affairs-and-critical-technology

Cyber Incident Victim: Fiji Government. (2021). Retrieved from CSIDB: https://www.csidb.net/csidb/incidents/b733145c-f192-4a9e-83ba-3e633eb21903/

Development Partners/Donor Profiles. (2025). Retrieved from USP: https://www.usp.ac.fj/dcu/donor-profiles/

Dziedzic, S. (n.d.). *Australia sends expert teams to Fiji as Chinese state-backed hackers attack Pacific Islands Forum*. Retrieved from ABC News: https://www.abc.net.au/news/2024-09-12/chinese-state-backed-hackers-attack-pacific-islands-forum/104341412

EBayShop Online Recruitment scam. (2023). Retrieved from FijiVillage: https://www.fijivillage.com/news/EBayShop-Online-Recruitment-scam-485fxr/

FIJI STRENGTHENS CYBERSECURITY WITH ESTABLISHMENT OF FIJI CERT AND NATIONAL STRATEGY. (2024, October). Retrieved from Fiji Gov: https://www.fiji.gov.fj/Media-Centre/News/FIJI-STRENGTHENS-CYBERSECURITY-WITH-ESTABLISHMENT

Fiji upholds China policing agreement, Guardian Australia reports. (2024). Retrieved from Reuters: https://www.reuters.com/world/asia-pacific/fiji-upholds-china-policing-agreement-guardian-australia-reports-2024-03-16/

Gil. (2021). *REvil/Kaseya Incident Update*. Retrieved from Cyberint: https://cyberint.com/blog/research/revil-kaseya-incident-update/?utm_source=chatgpt.com

James McBride, N. B. (2023). *China's Massive Belt and Road Initiative*. Retrieved from CFR: https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

Kumar, K. (2025, March). *Government steps up efforts to strengthen cybersecurity*. Retrieved from FBC: https://www.fbcnews.com.fj/news/government-steps-up-efforts-to-strengthen-cybersecurity/#:~:text=Among%20its%20key%20initiatives%2C%20the,Understanding%20on%20Cyber%20Security%20Cooperation.

MITRE. (2024). *REvil*. Retrieved from MITRE: https://attack.mitre.org/software/S0496/

Pratap, R. (2023). *Minister highlights Fiji's cybersecurity efforts*. Retrieved from FBC News: https://www.fbcnews.com.fj/news/minister-highlights-fijis-cybersecurity-efforts/

Sajid, I. (2022). *Australia hands over redeveloped Blackrock military training camp to Fiji*. Retrieved from AA: https://www.aa.com.tr/en/asia-pacific/australia-hands-over-redeveloped-blackrock-military-training-camp-to-fiji/2534521

Team, T. B. (2019). *Threat Spotlight: REvil/Sodinokibi Ransomware*. Retrieved from BlackBerry Blog: https://blogs.blackberry.com/en/2019/07/threat-spotlight-sodinokibi-ransomware?utm_source=chatgpt.com

Vucukula, E. (2024). *Scams worth $614k | CID investigates 650 online cases*. Retrieved from The Fiji Times: https://www.fijitimes.com.fj/scams-worth-614k-cid-investigates-650-online-cases/