Cyber Threat Advisory

03 September 2026

TLP:CLEAR

Redline Infostealer: Cyber Threat Advisory

This advisory is relevant to all Samoan individuals, businesses and organisations. This alert is intended to be understood by both general and technical audiences.

What is Redline Infostealer?

Redline Infostealer is currently one of the most prevalent information-stealing malware families operating across the Asia-Pacific region. It has been used in the Pacific to steal usernames, passwords, digital wallets (such as Apple or Google), financial information, and system data that can later be sold on criminal marketplaces or used in follow-on attacks such as ransomware and business email compromise attacks (BEC). Criminals have targeted:

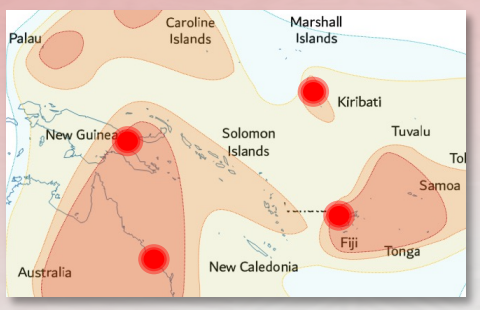
- Government Credentials
- Online Payment Services
- Banking and Financial Services Accounts
- Email Accounts
- Healthcare Patient Data
- Retail Platforms

Infostealer attacks provide a foothold for increasingly severe ransomware and malware attacks. Harvested credentials are sold on criminal forums, exposing citizens and organisations to further disruption.

How does this impact us?

INTERPOL has reported multiple infostealer attacks in our region.[1]

Kiribati **Fiji** **Papua New Guinea** **Australia**



New infostealer variants are emerging. Prior attacks have led to:

- Flow-on Ransomware Attacks
- Network Compromise
- Identity and Financial Theft
- Severe Data Breaches

How do we stay secure?

Implement Multi-Factor Authentication

This protects user access and prevents stolen passwords from being used in subsequent attacks.

Strengthen Email Security

Redline Infostealer uses phishing links and executable attachments, making properly configured phishing filters essential.

Disable Browser Password Storage

Redline can steal browser-saved credentials. Manually entered passwords or enterprise password managers are far safer alternatives.

Conduct Awareness and User Training

Provide regular training so staff can recognise emerging threats, indicators of compromise and system red flags.

If you have been affected by malware or have experienced a cyber incident, contact SamCERT on:

www.samcert.gov.ws/report-incident

samcert@mcit.gov.ws

+685 26 117

[1] INTERPOL, Asia and South Pacific Cyber Threat Assessment Report 2025/2026 (Singapore: INTERPOL, 2025), 26.

TLP:CLEAR