GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

10 July 2026

Advisory 164: Malware Network Infrastructure Indicators

Release Date: 09th July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

This is not a single software vulnerability advisory, but a malware C2/network infrastructure indicator package: 3,698 IP addresses actively associated with 19 distinct malware families over a 10-day observation window (22 June – 1 July 2026). These are network indicators of compromise (IOCs) — infrastructure known to be hosting command-and-control (C2), payload delivery, or data exfiltration for active malware campaigns.

CERTVU shares for cyber defense (detection/blocking) purposes only.

What are the systems affected?

The malware families represented span multiple platforms and functions:

- Windows infostealers/RATs
- macOS-targeting

- Combined backdoor/rootkit
- Supply-chain/dev-tooling
- Legacy backdoor/RAT

What does this mean?

How it's exploited:

Delivery and operating mechanisms vary by family but generally fall into these patterns:

- **Phishing-delivered droppers/loaders** (Amadey, Hancitor, VenomRAT, SocGholish) — malicious attachments, disguised purchase orders, or fake software update prompts trigger initial infection.
- **Loader-to-payload chains** (Bumblebee, Gootloader, Krampus, KOI Loader, PurpleFox) — an initial loader establishes a foothold, then pulls down infostealers, ransomware, or RATs from the flagged infrastructure.
- **Info-stealing over encrypted C2** (Redline, Raccoon, Vidar, StealC, Lumma, RisePro) — harvest browser credentials, cookies, crypto wallets, and system data, exfiltrating to the listed IPs.
- **RAT-based remote control** (AsyncRAT, DCRat, SparkRAT, HabitsRAT, Sectop_RAT) — full remote command execution, keylogging, and screen capture over C2 channels at the flagged addresses.
- **macOS-specific theft** (AMOS/Odyssey/MacSync/Cuckoo Stealer) — harvest local files, app data, and crypto wallets, often via trojanized utility apps.
- **Self-propagating supply-chain compromise** (GlassWorm) — spreads through developer tools/extensions using obfuscation and blockchain-based C2 to resist takedown.

Mitigation process

CERTVU recommends the following:

- **Ingest IOCs into detection tooling** — load the 3,698 IP addresses (by malware family, matching Elastic Fleet indices once your SIEM outage is resolved) into firewall/IDS/IPS blocklists and SIEM correlation rules, scoped to the observation window dates in the spreadsheet.
- **Retrospective log review** — search historical DNS, proxy, and firewall logs (22 June–1 July) for any outbound connections to the listed IPs; treat any hit as a probable compromise requiring full incident response.
- **Endpoint scanning** — run updated AV/EDR signatures for the 19 named families across Windows and macOS estates, particularly Amadey and Purplefox given their volume in this feed.
- **Email/phishing controls** — since several families rely on phishing (Agent Tesla, Hancitor, VenomRAT, SocGholish), reinforce attachment sandboxing and user awareness for disguised purchase orders/invoices and fake update prompts.

Reference

1. https://www.microsoft.com/en-us/security/blog/2026/06/24/stealc-and-amadey-breaking-down-infostealers-and-the-cybercrime-services-that-deliver-them/
2. https://www.trendmicro.com/en_us/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html