

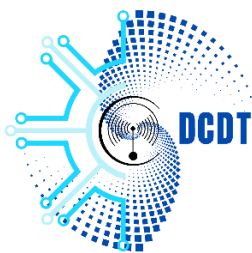
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

9 September 2026

Advisory 272: DYSPHOR1A Ransomware and Data-Extortion Group — Regional Threat Awareness.

Release Date: 9th September 2026

Impact: **MEDIUM — Preventive / Situational Awareness**

TLP: CLEAR

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

This alert is relevant to Government agencies, critical infrastructure operators, and private-sector organizations operating within Vanuatu's cyberspace, across all sectors. This alert is intended to be understood by both technical and non-technical readers, given its preventive and situational-awareness nature.

What is it?

CERTVU is issuing this advisory to raise awareness of DYSPHOR1A, a ransomware and data-extortion group that emerged in late August 2026 and has been actively compromising organisations across the Asia-Pacific region since. The group combines file encryption with data theft, operating a public leak site to pressure victims into payment (double extortion) if a ransom is not paid. This advisory is issued following a regional threat notification received from the Myanmar Cyber Emergency Response Team (mmCERT) and CERTVU's own review of publicly available threat intelligence.

Who is affected?

No Vanuatu-based organization has been identified as a victim of DYSPHORIA to date. However, given the group's demonstrated targeting of government agencies and critical services in the wider region.

CERTVU is issuing this advisory as a precautionary measure for all constituents operating within Vanuatu's cyberspace, including government agencies, critical infrastructure operators, and the private sector.

The sectors already targeted regionally by DYSPHORIA include government and defence, financial services, technology, transportation, education, and professional services hence this map closely onto sectors present in Vanuatu's own economy and public administration, reinforcing the precautionary basis for this advisory even in the absence of a confirmed local victim.

What does this mean?

Observed Tactics, Techniques, and Procedures (MITRE ATT&CK):

- Gaining or extending access using legitimate, compromised account credentials (Valid Accounts) rather than novel exploits.
- Moving across networks using Remote Desktop Protocol and other remote services (Remote Services / RDP).
- Spreading via shared network drives and folders by planting malicious content in shared locations (Taint Shared Content).
- Disabling or weakening security tools and monitoring prior to deploying its payload (Impair Defenses).
- Establishing persistence through autostart mechanisms triggered at boot or logon (Boot or Logon Autostart Execution).
- Executing malicious commands and scripts on compromised systems (Command and Scripting Interpreter).
- Encrypting data for impact and deleting or disabling backup and recovery mechanisms, including shadow copies, to hinder recovery (Data Encrypted for Impact; Inhibit System Recovery).

Indicators and further technical detail:

- Specific file hashes, command-and-control infrastructure, and ransom note samples associated with this group have not yet been made publicly available.
- CERTVU is engaging with regional partners, including mmCERT, to obtain and share further technical indicators as they become available; this advisory will be updated or supplemented if and when concrete indicators of compromise can be published.

Mitigation process

CERTVU recommends the following:

1. Enforce multi-factor authentication (MFA) on all remote access services
 - Enforce MFA on all remote access services, including VPNs and any Remote Desktop Protocol (RDP) access, and disable direct internet-facing RDP where not strictly required.
2. Monitor for anomalous RDP and remote-service logons, particularly outside of normal business hours or from unexpected source locations
3. Review and rotate privileged and service-account credentials
4. Apply network segmentation to limit lateral spread
5. Harden endpoint protection and security monitoring
6. Maintain regular, tested, offline or immutable backups
7. Apply timely patching and maintain up-to-date asset inventories

Report any suspected compromise, unusual account activity, or ransomware-related indicators to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. [SOCRadAr Ransomware Intelligence — DYSPHOR1A Group Profile:](https://socradar.io/free-tools/ransomware-intelligence/groups/dysphor1a)
<https://socradar.io/free-tools/ransomware-intelligence/groups/dysphor1a>
2. Myanmar Cyber Emergency Response Team (mmCERT) - Regional Threat Intelligence Notification, September 2026 (correspondence; not publicly available)
3. [Ransomware.live — DYSPHOR1A group leak-site tracking:](https://www.ransomware.live/group/DYSPHOR1A)
<https://www.ransomware.live/group/DYSPHOR1A>