# CYBERSECURITY ALERT/ ADVISORY

## Alert Status: High

### Hackers Targeting Linux Systems with New Malware

The Department of Information and Communications Technology (DICT), through the National Cyber Security Center (NCSC), issues this advisory to alert all PNG Government departments, agencies, and organizations about a sophisticated cyber threat targeting Linux systems.

Recent reports indicate that hackers are actively targeting Linux systems using newly discovered malware. This campaign focuses on exploiting vulnerabilities to gain unauthorized access, steal sensitive data, and maintain persistence in compromised networks.

**Threat Overview**

- **Targets:** Linux servers and workstations, particularly in government, critical infrastructure, and technology sectors.

- **Attack Vector:** Exploitation of unpatched vulnerabilities and deployment of custom malware.

- **Malware Capabilities:**

- Remote command execution
- Data exfiltration
- Persistence mechanisms to evade detection

**Affected Systems**

Linux-based systems, particularly those running:

- Connectwise ScreenConnect
- F5 BIG-IP
- Ivanti Cloud Service Appliance (CSA)

To protect your systems from this threat, the NCSC recommends the following measures:

1. **Patch Management:** Apply the latest security patches to all affected systems, particularly for Connectwise ScreenConnect, F5 BIG-IP, and Ivanti CSA.

2. **System Hardening:**

- Disable unnecessary services and ports.

- Enforce strict access controls and use the principle of least privilege.

3. **Monitoring and Detection:**

- Deploy intrusion detection systems (IDS) and endpoint detection and response (EDR) solutions to identify suspicious activities.

- Monitor for unusual network traffic or unauthorized access attempts.

4. **Incident Response:**

- Review system logs for signs of compromise.

- Isolate affected systems and conduct forensic analysis if an intrusion is suspected.

5. **User Awareness:** Educate staff about phishing and social engineering tactics that may be used to deliver malware.

For more detailed information and specific indicators of compromise (IOCs), refer to the full report by The Hacker News.

Timely response to these threats is imperative to maintain the integrity and security of organizational systems and critical data. Proactive vigilance and consistent infrastructure maintenance are essential components of an effective cybersecurity posture.

The National Cyber Security Center (NCSC), in collaboration with the Department of ICT, remains committed to fostering a robust digital security framework. We strongly urge all stakeholders to implement the prescribed mitigation measures to strengthen collective cyber resilience.

For additional support or technical inquiries, please contact the NCSC through official channels. Through coordinated efforts and sustained commitment to cybersecurity best practices, we can collectively safeguard Papua New Guinea's digital ecosystem.