CERT Tonga

Ministry of Meteorology Energy
Information, Disaster Management,
Environment, Communications and
Climate Change

Inc Ransomware and Affiliate Network Operating in the Blue Pacific

This advisory outlines the activity of ransomware group Inc Ransomware and their affiliate network, and the threat their operations currently pose to networks hosted in the Blue Pacific. This alert is intended to be understood by technical users. Organisations and agencies within the Blue Pacific are encouraged to apply available mitigations as soon as possible.

What's Happened?

Inc Ransomware provides a sophisticated ransomware-as-a-service operation to its affiliate network. Affiliate members use this ransomware to target victims, encrypting vital information before directing their victims to a Dark Web site or demanding payment in exchange for a decryption key. While affiliate members distribute the ransomware, Inc Ransomware themselves are also involved in the extortion of their victims and in handling payments. Their strategy primarily targets high-value entities handling sensitive data, with activity suggesting a trend towards disproportionately targeting healthcare providers.

Inc Ransomware group and their affiliate network have previously targeted the United States and United Kingdom, but recently the have been observed increasingly operating within the Blue Pacific.

How do I stay secure?

CERT Tonga advises that organisations and Government Ministries implement the following controls to **detect** INC Ransomware and affiliate activity, and to **protect your organisation from this threat**:

Enhancing Detection:

1. Review Firewall for evidence of potentially suspicious IP's, brute force attacks, vulnerability exploitation or port scanning that may indicate malicious activity.
2. Detecting Unauthorised Remote Access and Remote Management Tools that are commonly invoked by ransomware groups.
3. Centralise Logging and alerting (i.e. EDR & SIEM), enabling early warnings while also ensuring logs are retained for an appropriate period to support with forensic efforts.
4. Monitor the use of Generic Accounts and where possible prevent administrators from using generic accounts.
5. Threat Hunt for indicators of INC ransomware including for anomalous activity in system event logs, stored network traffic logs and endpoint logs that align with the tactical techniques and procedures (TTPs) and IOCs outlined in public Inc Ransomware intelligence reports.

Mitigating Controls:

1. Ensure backups of critical systems are captured and tested, ideally these backups are kept separate, in a different location, from your network and systems.
2. Review and restrict activity entering and leaving your network by locking down your Firewall settings to restrict traffic accepted into and leaving from the network.
3. Review your VPN settings, restricting what resources, servers and applications can be accessed while using the VPN.
4. Lock down all remote management tools, including TeamViewer and AnyDesk, for example.
5. Implement Multi-Factor Authentication (MFA) on all end-points, applications, accounts and services.
6. Robust patch management, ensuring software and systems are up-to-date with security patches that are critical to closing the potential vulnerabilities exploited by ransomware actors.

Where can I go for help?

If you suspect you have been impacted by this ransomware threat, or If you require assistance / advice on how to respond to this alert, please contact CERT Tonga directly:

CERT Tonga Ministry of MEIDECC Nuku'alofa Tel: 2378 (CERT) Email: cert@cert.gov.to Web: https://cert.gov.to/ Twitter: @CERTTonga | Facebook: @CERTTonga