CERT Tonga

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

Information Stealer (Infostealer) Malware Advisory

This advisory is relevant to all Tongan individuals, businesses and organisations. This alert is intended to be understood by both general and technical. Individuals and organisations are encouraged to remain vigilant and aware of Infostealer activity, and to apply available mitigations as soon as possible. Implementing mitigation controls is especially important due to the stealthy nature of this malware type, and its ability to remove itself from devices following successfully stealing data.

What's Happened?

Infostealer malware continues to be one of the most common avenues of cyber-attack in the Pacific. The goal of this information stealing malware is to compromise personal information, including:

- *usernames and passwords*
- *personal documents and images*
- *contents of digital communications (including messaging and email)*
- *technical computer and web browser information.*

Cybercriminals then use this information to impersonate victims or sell it for monetary gain. The purchase of this stolen information by downstream threat actors (such as ransomware gangs) means it can later be leveraged as part of future attacks. This introduces a risk of identity theft, financial fraud, extortion, and taking over of accounts.

How do I stay secure?

CERT Tonga advises that individuals and organisations implement the following controls to **detect** information stealer malware and to **limit its effectiveness**:

Enhancing Detection: *Indications that you've been impacted by Infostealer malware include observing:*

1. Suspicious activity on your accounts, such as altered settings, unusual login patterns, password changes, and having access to those accounts blocked.
2. Unauthorised and unexpected bank account transactions.
3. An increased volume in unexpected or spam communications (including calls and emails), or increased communications from organisations that you have not interacted with before.

Mitigating Controls: *Reduce the likelihood of information stealers in your environment:*

1. Use passwords on all devices and accounts, ensuring that these passwords are distinct, complex, and long.
2. Implement Multi-Factor Authentication (MFA) on all devices and accounts.
3. Be cautious when clicking on links in emails, messages, and advertisements online, especially if they're not from official or reputable sources.
4. Ensure that software is only downloaded from trusted sources. Pirated software or files from unknown sources are a common method of spreading Infostealer malware, so ensure to avoid these.
5. Use trusted antivirus software on your devices, ensuring that it is regularly updated.

For more guidance, please refer to the advisory from the Australian Cyber Security Centre.

Where can I go for help?

If you suspect you have been impacted by information stealer malware, 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

TLP:CLEAR