CERT Tonga

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

TLP: White[1]

Advisory- Spike in Ryuk Ransomware Observed

Dear Constituents,

CERT Tonga is aware of noticeable occurrences of Ryuk ransomware observed. These incidents have been mostly reported in the United States (US) health care sector. The intensity of the incidents have lead to a joint cybersecurity advisory by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS).

Although it has not been confirmed that it is only specifically targeting the Health Sector in the US, but this campaign is a grave concern for CERT Tonga. Ryuk ransomware has been known to be spread via Emotet, and Emotet has been widely observed in Tonga and the region.

How it Works

Ryuk is a type of crypto-ransomware that uses encryption to block access to a system, device, or file. Ryuk is often dropped on a system by other malware, most notably TrickBot which gains access to a system via Remote Desktop Services. Ryuk demands payment via Bitcoin crypto-currency and directs victims to deposit the ransom in a specific Bitcoin wallet.

Ryuk is primarily spread via other malware dropping it onto an existing infected system. Ryuk ransomware attacks occur in 3 ways:

1. Through Emotet or Trickbot infection.
2. Through email attachments that deploy Ryuk ransomware directly.
3. Through RDP access, an attacker can install and execute Ryuk directly on the target machine.

What to do

- Ensure that you have a working backup of crytical systems and files as well as maintaining an offline backup.
- Make sure you have an anti-virus solution installed and kept up to date with detection signatures.
- Implement multi-factor authentication for account access where possible.
- Keep systems up-to-date with patches.
- Disable any unnecessary remote access capabilities (such as RDP).

[1] CERT Tonga adopts the Traffic Light Protocol

Reference

- https://us-cert.cisa.gov/ncas/alerts/aa20-302a#https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- https://www.cert.govt.nz/it-specialists/advisories/increase-in-ryuk-ransomware-attacks/
- https://www.cyber.gov.au/acsc/view-all-content/advisories/2019-131a-emotet-malware-campaign-recommended-actions

Please for more information you can contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga

Disclaimer Notice:
The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services.