Cyber Threat Advisory

11 February 2025

TLP:CLEAR

Advanced Persistent Threat 40 (APT40) Advisory

This advisory outlines the activity of a sophisticated cyber group and the threat they currently pose to networks hosted in the Blue Pacific. The advisory draws on both the Samoa National Computer Emergency Response Team's (SamCERT) investigations and insights shared by other partner countries that have reported extensively on this threat actor.

APT40 is a state-sponsored cyber group that utilises advanced capabilities to conduct malicious cyber operations against government and key critical infrastructure (CI) systems. This group has previously targeted the United States, Australia, and has most recently been observed conducting operations directed at the sensitive networks administered by Pacific Island nations.

What does the actor do?

APT40 has a track-record of targeting government and private sector networks globally, however recent activity observed by SamCERT suggests the existence of campaigns specifically targeting networks hosted in the Blue Pacific. SamCERT has analysed APT40 activity consisting of stealthy fileless malware using previously unobserved registry loading techniques. In addition, we have also observed secondary loaders consisting of modified commodity malware that allows the threat actor to maintain persistence and command and control in the network. These malwares are used together to avoid detection and enable the exfiltration of sensitive data from Blue Pacific networks. It is essential to note that throughout our investigations we have observed the threat actor pre-positioning themselves in the networks for long periods of time and remaining undetected before conducting exfiltration activity. This activity is sophisticated, and the methodologies employed by APT40 across our investigations can be summarised as follows:

- **Delivery of malware** through side-loading malicious DLL files and using the execution of legitimate programs to load their malware. Further malware delivery occurs through registry modifications.
- **Persistence** is often sort by the creation of scheduled tasks, and delivery of existing modified malware to provide remote access and command and control capabilities.
- **Lateral Movement** to facilitate reconnaissance/ mapping across networks often with the goal of identifying high profile targets.
- **Living off the land** techniques are often used, including deployment or use of common administrative tools to move and stage data.
- **Staging and Exfiltration** of target data via modified reverse proxies to deliberately conceal traffic to the command-and-control infrastructure.
- **Detection evasion techniques** by executing malware in memory, as well as other techniques including removing indicators, timestamping, software packing, deleting logs, obfuscation and masquerading.

How do I stay secure?

SamCERT advises that organisations and government ministries review the following to determine their exposure to APT40:

- **Undertake systematic threat hunting** across your environment for evidence of APT40 activity. Ensure that appropriate logging is enabled to assist in investigation activities. Organisations are encouraged to work with SamCERT to complete this activity.
- **Immediately Review the Patching Status** of all your key assets, including endpoints and firewalls, to prevent the actor's ability to break into your environment. Consider undertaking vulnerability scans of your environment to determine key weaknesses.
- **Review and Update Incident Response plans** to ensure that your orgnaisation is adequately prepared to respond to an advanced cyber event.

Where can I go for help?

If you suspect you have been impacted by APT40 we encourage you to submit a report at: www.samcert.gov.ws/report-incident

If you require more information, please contact SamCERT: samcert@mcit.gov.ws +685 26 117

TLP:CLEAR