Press release

July 9, 2024
National Center of Incident Readiness and Strategy for Cybersecurity
National Police Agency

Co-sealing the Australian-Led International Advisory on the APT40 group

1. Overview

On July 9, the National Center of Incident Readiness and Strategy for Cybersecurity and the National Police Agency (NPA) co-sealed and published an international advisory entitled "APT40 Advisory PRC MSS Tradecraft in Action" (hereinafter referred to as the "Advisory"). The Advisory was prepared by the Australian Cyber Security Centre (ACSC) under the Australian Signals Directorate (ASD). Tentative translations will be released as soon as possible.

Following eight countries co-sealed the Advisory and are listed as co-authoring organizations: Australia, the United States, the United Kingdom, Canada, New Zealand, Germany, South Korea, and Japan.

In Japan, it has been confirmed that Japanese companies had also been targeted by a group conducting cyberattacks known as APT40.

The Advisory analyzes past incidents in Australia by APT40, details their attack techniques as case studies, and provides measures for detecting and mitigating these attacks. Given its contribution to strengthening cybersecurity in Japan, we have decided to co-seal it.

We will continue our efforts to strengthen international cooperation in the field of cybersecurity.

2. Overview of the Advisory

(1) The Advisory provides an outline of People’s Republic of China(PRC) state-sponsored cyber groups and the threats posed to Australian networks by these groups. These cyber actors are understood to be associated with the Chinese Ministry of State Security (MSS). Their activities and techniques overlap with those of the group tracked as APT40. This group is understood to be based in Haikou City, Hainan Province, receiving tasking from the MSS Hainan State Security Department.

(2) APT40 has repeatedly targeted Australian networks as well as government and private sector networks, and the threat is ongoing. Notably, APT40 possesses the capability to rapidly transform and adapt exploit proof-of-concept(s) (POCs) of new vulnerabilities and immediately utilise them against target networks.

(3) APT40 prefers exploiting vulnerable, public-facing infrastructure and places a high priority on obtaining valid credentials. APT40 regularly uses web shells for persistence, and focuses on establishing persistence. However, as persistence occurs early in an intrusion, it is more likely to be observed in all intrusions.

(4) Although APT40 has previously used compromised Australian websites as command and control (C2) hosts for its operations, the group has embraced the global trend of using compromised devices, including small-office/home- office (SOHO) devices, as

operational infrastructure and last-hop redirectors for its operations in Australia. This technique is also regularly used by other PRC state-sponsored actors worldwide.

(5) Two APT40 attack-related incidents as case studies;

(a) Case Study 1 - The actors compromised the network of an organization in Australia from July to September 2022 and deployed a web shell. Subsequently, the actors laterally moved across the networks to access sensitive data, including privileged authentication credentials.

(b) Case Study 2 - The actors compromised the network of an organization in Australia from April 2022 and exfiltrated several hundred unique username and password pairs, a number of multi-factor authentication codes, and technical artifacts related to remote access sessions on the compromised appliance.

(6) The Advisory strongly recommends implementing the ASD "Essential Eight" Controls. The following measures are particularly important for detecting and mitigating attacks.

(a) The files identified in APT40 attack incidents are stored in locations accessible to all user accounts registered in Windows with write permissions enabled. Anomalous activity can be detected by setting rules to identify process executions from such suspicious locations.

(b) Mitigations

(i) Logging: Ensure web server request logs, Windows event logs, and proxy logs are stored appropriately.

(ii) Patch management: Ensure all internet exposed devices, such as web servers and remote access gateways, have security patches or mitigations applied within 48 hours. Use the latest versions of software and operating systems where possible.

(iii) Network segmentation: Segmenting networks limits or blocks lateral movement for adversaries. Important servers such as Active Directory and other authentication servers should only be able to be administered from a limited number of intermediary servers or "jump servers" and these servers should be closely monitored, be well secured and limit which users and devices are able to connect to them.

(iv) Other measures

- Disable unnecessary network services, ports, and protocols.
- Use well-tuned web application firewalls (WAFs).
- Enforce least privilege.
- Use multi-factor authentication (MFA) and managed service accounts to make credentials harder to crack and reuse.
- Replace end-of-life equipment.

(End)