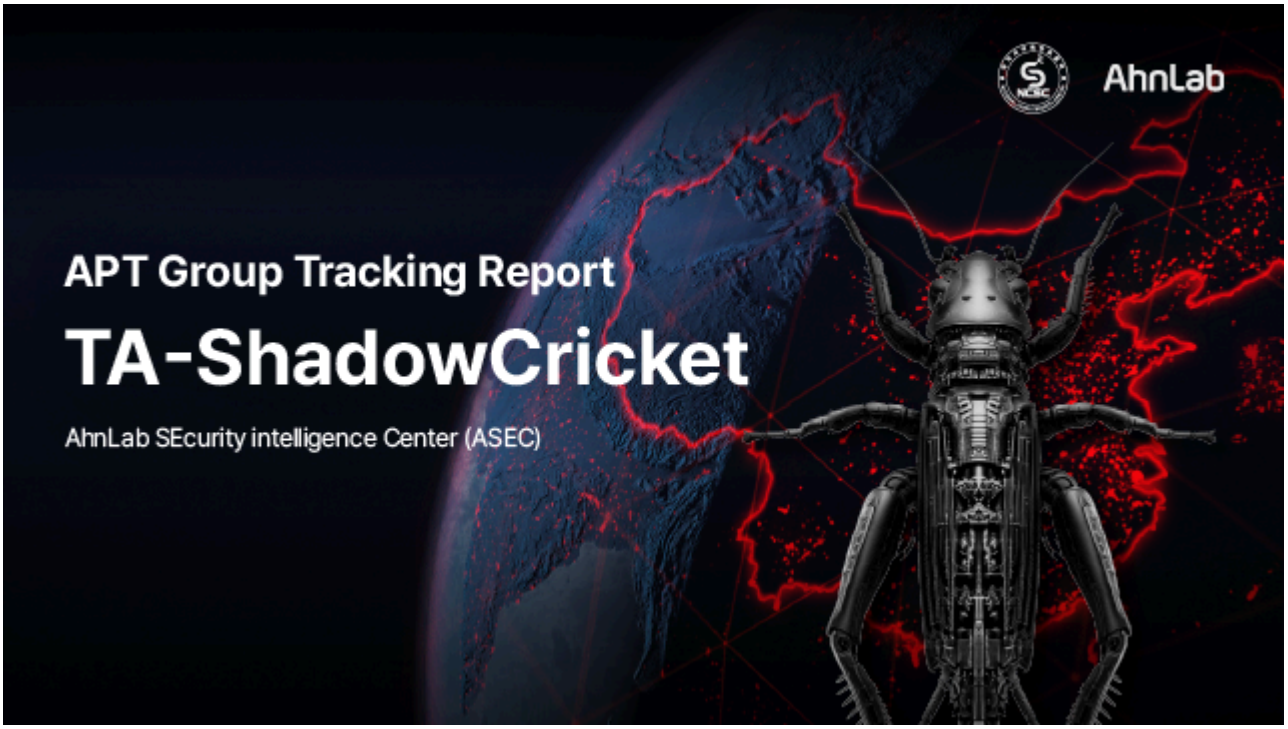
TA-ShadowCricket: The 13-Year Shadow Campaign Exposed

Archived: 2026-04-05 16:17:44 UTC



▶ Download Full Report

Background

TA-ShadowCricket is a threat group formerly known as Shadow Force and is suspected to have ties to China. This group has been active for over ten years in countries across the Asia-Pacific region, including South Korea. The group primarily infiltrates systems by using Windows MS SQL and RDP, and installs IRC bots or backdoors for control. Since December 2021, installations of virtual asset miners have also been identified on some compromised systems.

This report is based on joint tracking of TA-ShadowCricket's activities since 2023, conducted by the National Cyber Security Center (hereinafter referred to as NCSC) and AhnLab.

TA-ShadowCricket

Threat Group Naming

AhnLab manages threat activity using its Threat Actor Classification System and Naming Convention, which categorizes threats into four levels. Threat actors are classified as either unidentified (Larva) or identified (Arthropod).

Since November 2024, AhnLab has been analyzing the threat group's IRC server and related malware in collaboration with the NCSC. At that time, the threat group was being tracked as the unidentified threat actor Larva-24013. It was later confirmed that they were connected to the previously known Shadow Force group. Accordingly, in line with AhnLab's classification system and naming convention, the group was newly designated as the identified threat actor TA-ShadowCricket.

Conclusion

The TA-ShadowCricket group has been operating out of Korea for over a decade, targeting regions across Asia. The threat actors have maintained their legacy attack habits as they have consistently used the same malware and tool file names. Despite this, there has been limited coverage of this threat group by security firms or institutions, resulting in a continued lack of information.

TA-ShadowCricket does not demand ransom post-breach, nor does it release stolen data on the dark web. Instead, the group has quietly operated for over 13 years, persistently managing affected systems and their corresponding C2 servers across thousands of IPs. This infrastructure could potentially be leveraged for future attacks such as DDoS.

Various indicators—including the tools and developers used, primary target regions, and connections to C&C servers via Chinese IPs—suggest potential links to China. However, the use of personal nicknames within the malware and recent behaviors like installing miners raise doubts about whether this is a state-sponsored APT group.

This joint analysis has confirmed that TA-ShadowCricket still manages compromised systems using IRC bots. Analysis of the IRC servers indicates that more than 2,000 bots are currently in operation. To prevent further, potentially widespread damage, it is critical to block these IRC servers and to detect, neutralize, and remove the associated malware.

▶ Download Full Report

Source: https://www.ahnlab.com/en/contents/content-center/35891