China-Linked Group TAG-28 Targets India's "The Times Group" and UIDAI (Aadhaar) Government Agency With Winnti Malware

recordedfuture.com/blog/china-linked-tag-28-targets-indias-the-times-group

Blog

Insikt Group®

Editor's Note: *The following post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*

Executive Summary

India continues to bear the brunt of hostile cyber operations from Chinese state-sponsored groups. Earlier this year, Insikt Group documented a RedEcho campaign targeting India's critical national infrastructure following a rapid deterioration in bilateral relations after both countries clashed on the China-India border. We also recently identified renewed RedFoxtrot operations targeting an Indian state-owned enterprise involved in the nuclear, space, and defense sectors.

Following this theme of Chinese targeting of Indian entities, we have identified further suspected intrusions targeting the Indian media conglomerate Bennett Coleman And Co Ltd (BCCL), commonly known as "The Times Group"; the Unique Identification Authority of India (UIDAI); and the Madhya Pradesh Police department. The UIDAI is the Indian government agency responsible for the national identification database, more commonly called "Aadhaar", which contains private biometric information for over 1 billion Indian citizens. These intrusions were conducted by an activity group we track using a temporary designation, TAG-28.

Chinese state-sponsored intrusions targeting news outlets is not a recent phenomenon. In 2013, the New York Times, the Washington Post, and Bloomberg News were targeted by a Chinese group in a widespread intelligence-gathering operation following a series of published articles that were perceived as presenting China unfavorably. Subsequently in 2014, pro-democracy news outlets in Hong Kong were targeted during the Umbrella Movement protests. TAG-28's Winnti campaign targeting BCCL is the latest in a long line of targeted intrusions against international media outlets.

Key Judgments

- TAG-28 highly likely targeted UIDAI due to its ownership of the Aadhaar database. Bulk personally identifiable information (PII) data sets are valuable to state-sponsored threat actors. Likely uses of such data include, but are not limited to, identifying high-value targets such as government officials, enabling social engineering attacks, or enriching other data sources.
- Given the reach of The Times Group publications and their consistent reporting on the "India China war", TAG-28's targeting of BCCL is likely motivated by wanting access to journalists and their sources as well as pre-publication content of potentially damaging articles focusing on China or its leadership.
- It is less likely that TAG-28 would gain access to media entities to interfere with publishing platforms by changing or disrupting articles supporting Chinese information operations.
- As of early August 2021, Recorded Future data shows a 261% increase in the number of suspected state-sponsored Chinese cyber operations targeting Indian organizations and companies already in 2021 compared to 2020. This follows an increase of 120% between 2019 and 2020, demonstrating China's growing strategic interest in India over the past few years.

Editor's Note: *This post was an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*

Related