

Security firm links cyber spy campaign to Chinese hacker

March 30 2012



Tokyo-based computer security firm Trend Micro on Friday said it linked a hacker in China to a "cyber espionage" campaign targeting India, Japan, and Tibetans.

Tokyo-based computer security firm Trend Micro on Friday said it linked a hacker in China to a "cyber espionage" campaign targeting India, Japan, and Tibetans.

A Chinese hacker whose nicknames include "Dang0102" and "scuhkr" was involved in online spying to steal [military secrets](#), spy on Tibetan activists and mine information from players in the energy, shipping and [aerospace industry](#).

"The Luckycat campaign attacked a diverse set of targets using a variety of malware, some of which have been linked to other cyber-espionage

campaigns," Trend Micro said in a research paper.

"We were able to track elements of this campaign to hackers based in China."

LuckyCat has been going on at least since June of 2011 and has been linked to 90 [cyber attacks](#) in Japan and India and on Tibetan activists, according to Trend Micro.

Cyber spies compromised 233 computers, usually by tricking users into opening links or files booby-trapped with [malicious software](#) crafted to let hackers continually loot information, the security company said.

The pinpointed LuckyCat hacker has published posts in a notorious XFocus online forum and recruited peers to join a network attack and defense project at the Sichuan University Information Security Institute, according to Trend Micro.

Trend Micro refused to comment on reports that the hacker was a former graduate student who works for China's leading Internet portal Tencent.

The report did not directly implicate the Chinese government, but [security researchers](#) believed that the style of the attacks and the types of targets indicated state-sponsored spying.

"Unlike largely indiscriminate attacks that focus on stealing credit card and banking information associated with cybercrime, targeted attacks noticeably differ and are better characterized as cyber espionage," Trend Micro said.

(c) 2012 AFP

Citation: Security firm links cyber spy campaign to Chinese hacker (2012, March 30) retrieved 10 September 2024 from <https://phys.org/news/2012-03-firm-links-cyber-spy-campaign.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.