

Bank hackers linked to wider campaign: researchers

27 May 2016

The hackers behind the \$81 million heist from the Bangladesh central bank have likely been involved in a series of attacks on the financial system, a US security firm has concluded.

Researchers at the security firm Symantec also found that the malware used in the bank hacks shares code with that used in the massive 2014 cyberattack against Sony Pictures.

Symantec said a bank in the Philippines has been attacked by the group that hit the Bangladesh central bank and attempted a heist from the Tien Phong Bank in Vietnam.

"Malware used by the group was also deployed in targeted attacks against a bank in the Philippines. In addition to this, some of the tools used share code similarities with malware used in historic attacks linked to a threat group known as Lazarus," Symantec researchers said in a blog post Thursday.

"The attacks can be traced back as far as October 2015, two months prior to the discovery of the failed attack in Vietnam, which was hitherto the earliest known incident."

News of the Bangladesh incident sparked a warning from the global financial interbank platform SWIFT, which earlier this month warned of a wide-ranging campaign.

SWIFT said this month that hackers exploited vulnerabilities at two unnamed banks to gain access to their fund transfer systems, which then give instructions to the SWIFT network.

Symantec said the [malware](#) found has been tied to the group known as Lazarus, blamed for the Sony attack which according to US officials had been ordered by North Korea.

"The discovery of more attacks provides further

evidence that the group involved is conducting a wide campaign against financial targets in the region," Symantec said.

"While awareness of the threat posed by the group has now been raised, its initial success may prompt other attack groups to launch similar attacks. Banks and other financial institutions should remain vigilant."

© 2016 AFP

APA citation: Bank hackers linked to wider campaign: researchers (2016, May 27) retrieved 26 June 2019 from <https://phys.org/news/2016-05-bank-hackers-linked-wider-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.