White House hackers 'Russian speakers': researchers

April 22 2015

Hackers who penetrated the State Department and White House computer networks in recent month were "Russian speakers," security researchers said Wednesday.

The hackers have aimed at high-profile targets including US government and commercial networks as well as in Germany, South Korea and Uzbekistan, according to researchers at Kaspersky Lab, a Russian-headquartered security firm.

The malware used, dubbed "CozyDuke," bears similarities to other malicious programs used in recent years and is designed to get around most detection programs.

Kaspersky said CodyDuke's coding is related to similar malware MiniDuke and CosmicDuke.

"We have been monitoring both MiniDuke and CosmicDuke for couple of years. Kaspersky Lab was the first to warn about MiniDuke attacks in 2013, with the oldest known samples for this cyberthreat dating back to 2008," said Kaspersky researcher Kurt Baumgartner.

"CozyDuke is definitely connected to these two campaigns, as well as to the OnionDuke cyberespionage operation. Every one of these threat actors continues to track their targets, and we believe their espionage tools are all created and managed by Russian-speakers."

According to Kaspersky, this group is responsible for the attack on the State Department which allowed hackers to access the White House.

Last year, White House officials acknowledged a computer intrusion but said no classified data was accessed, and did not comment on reports linking the attack to Russian hackers.

Kaspersky said a key element of the attacks was the use of "spearphishing," or emails that appear legitimate but contain attachments that install malware when a recipient clicks on them.

One of the attachment was an amusing "office monkeys" video which appears to be innocent.

"These videos are quickly passed around offices with delight while systems are infected in the background silently," the Kaspersky report said.

© 2015 AFP

Citation: White House hackers 'Russian speakers': researchers (2015, April 22) retrieved 19 April 2024 from https://phys.org/news/2015-04-white-house-hackers-russian-speakers.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.