The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Global Cyberespionage Network Uncovered by Kaspersky

By The Moscow Times

June 05, 2013



Computer security company Kaspersky Lab said its experts have uncovered a global cyberespionage campaign, which may have been in existence for nearly a decade and compromised more than 350 computer systems in 40 countries.

The malicious NetTraveler surveillance toolkit has been active since as early as 2004, but its activity peaked between 2010 and 2013. The initial attack begins with spear-phishing emails with malicious attachments that use vulnerabilities in Microsoft Office to compromise systems.

"The NetTraveler group's main domains of interest for cyberespionage activities include space exploration, nanotechnology, energy production, nuclear power, lasers, medicine and communications," Kaspersky Lab said in a statement.

Users and organizations in Mongolia and Russia were the hardest affected, followed by India,

Kazakhstan, Kyrgyzstan, China, Tajikistan, South Korea, Spain and Germany.

Kaspersky Lab's experts estimate the amount of stolen data stored on NetTraveler's command and control servers at more than 22 gigabytes.

"Exfiltrated data from infected machines typically included file system listings, keyloggs, and various types of files including PDFs, excel sheets, word documents and files," Kaspersky Lab said.

In addition, the NetTraveler toolkit was able to install additional info-stealing malware, such as a backdoor.

Original url:
https://www.themoscowtimes.com/2013/06/05/global-cyberespionage-network-uncovered-by-kaspersky-a24683