Kaspersky boss warns of emerging cybercrime threats

October 3 2015

Eugene Kaspersky, CEO of Kaspersky Lab, speaks in Washington on June 4, 2013

Russian online security specialist Eugene Kaspersky says cybercriminals will one day go for bigger targets than PCs and mobiles, sabotaging entire transport networks, electrical grids or financial systems.

The online threat is growing fast with one in 20 computers running on Microsoft Windows already compromised, the founder and [chief executive](link) of security software company Kaspersky Lab told AFP this week on the sidelines of a cybersecurity conference in Monaco.

QUESTION: How do cybercriminals work?

ANSWER: For every new device or operating system, there are hackers who will try to show off their skills by breaching its security, Kaspersky said.

"And then the criminals come," he said.

Cybercriminals break into systems by using the holes exposed by hackers, he added. Once in, they seek [personal financial data](link); encrypt corporate computers so as to get a ransom for their release; and infect computers with "botnet" software that makes the machines infect yet more victims.

"Today we see more than 300,000 unique attacks every day," Kaspersky said. "Five percent of all computers in the world connected to the Internet running with Windows are infected."

QUESTION: As an average user of the Internet, should I be worried?

ANSWER: You need to be aware of the threats and take care to avoid being an "easy victim", Kaspersky said, stressing that it is not just a question of installing [security software](link).

"It's like everyday life. If you just stay at home and if you don't have visitors, you are quite safe. But if you like to walk around to any district of your city, you have to be aware of their street crimes. Same for the Internet."

QUESTION: What is the next likely target for cybercriminals?

ANSWER: The big fear is that extremist groups hire hackers to compromise entire infrastructure networks, Kaspersky said.

"The next step is cyber sabotage, attacks on physical infrastructures and critical data," he said.

"They will target transportation infrastructures, electric grids, financial data, healthcare systems," he warned.

© 2015 AFP