Hackers target CEOs in 'Darkhotel' scheme

November 10 2014

In a new hacking scheme targeted at luxury hotels, those responsible are able to compromise hotel Wi-Fi networks and then trick executives into downloading malicious software that can allow their information to accessed remotely

Hackers have developed a scheme to steal sensitive information from top executives by penetrating the Wi-Fi networks of luxury hotels, security researchers said Monday.

A report by Kaspersky Lab said the "Darkhotel" espionage effort "has lurked in the shadows for at least four years while stealing sensitive data

from selected corporate executives traveling abroad."

Kaspersky said about 90 percent of the infections appear to be located in Japan, Taiwan, China, Russia and South Korea, but that the executives targeted include those traveling from the United States and other countries.

"The infection count numbers in the thousands," the report said.

"The more interesting traveling targets include top executives from the US and Asia doing business and investment in the (Asia-Pacific) region."

The hackers are able to compromise hotel Wi-Fi networks, and to then trick executives into downloading malicious software that can allow their information to accessed remotely.

"These tools collect data about the system and the anti-malware software installed on it, steal all keystrokes, and hunt for cached passwords in Firefox, Chrome and Internet Explorer; Gmail Notifier, Twitter, Facebook, Yahoo and Google login credentials; and other private information," the report said.

"Victims lose sensitive information—likely the intellectual property of the business entities they represent. After the operation, the attackers carefully delete their tools from the hotel network and go back into hiding."

Kaspersky researcher Kurt Baumgartner said the attacks are highly sophisticated.

"This threat actor has operational competence, mathematical and crypto-analytical offensive capabilities, and other resources that are sufficient to abuse trusted commercial networks and target specific victim

categories with strategic precision," he said.

Targets have included corporate chief executives, senior vice presidents, sales and marketing directors and top research staff at companies in the electronics, defense manufacturing, finance, automotive and pharmaceutical industries, among others. Some law enforcement, military and non-governmental officials have also been targeted.

"From our observations, the highest volume of offensive activity on hotel networks started in August 2010 and continued through 2013, and we are investigating some 2014 hotel network events," Kaspersky said.

The researchers said the risk can be mitigated by using a virtual private network that protects data.

The security team said that travelers should be extra cautious about software updates and should use software with protection against a broad range of threats in addition to viruses.

Citation: Hackers target CEOs in 'Darkhotel' scheme (2014, November 10) retrieved 20 June 2024 from https://phys.org/news/2014-11-hackers-ceos-darkhotel-scheme.html