Researchers predict new computer security threat for wireless networks: Typhoid adware (w/ Video)

May 21 2010

John Aycock (left) and student Daniel Medeiros Nunes de Castro have predicted a new computer security threat: Typhoid adware. Credit: Leanne Yohemas, University of Calgary

There's a potential threat lurking in your internet café, say University of Calgary computer science researchers. It's called Typhoid adware and works in similar fashion to Typhoid Mary, the first identified healthy carrier of typhoid fever who spread the disease to dozens of people in the New York area in the early 1900s.

"Our research describes a potential computer security threat and offers some solutions," says associate professor John Aycock, who co-authored a paper with assistant professor Mea Wang and students Daniel

Medeiros Nunes de Castro and Eric Lin. "We're looking at a different variant of adware - Typhoid adware -which we haven't seen out there yet, but we believe could be a threat soon."

Adware is software that sneaks onto computers often when users download things, for example fancy tool bars or free screen savers, and it typically pops up lots and lots of ads. Typhoid adware needs a wireless internet café or other area where users share a non-encrypted wireless connection.

"Typhoid adware is designed for public places where people bring their laptops," says Aycock. "It's far more covert, displaying advertisements on computers that don't have the adware installed, not the ones that do."

The paper demonstrates how Typhoid adware works as well as presents solutions on how to defend against such attacks. De Castro recently presented it at the EICAR conference in Paris, a conference devoted to IT security.

Typically, adware authors install their software on as many machines as possible. But Typhoid adware comes from another person's computer and convinces other laptops to communicate with it and not the legitimate access point. Then the Typhoid adware automatically inserts advertisements in videos and web pages on the other computers. Meanwhile, the carrier sips her latté in peace - she sees no advertisements and doesn't know she is infected ¬- just like symptomless Typhoid Mary.

U of C researchers have come up with a number of defenses against Typhoid adware. One is protecting the content of videos to ensure that what users see comes from the original source. Another is a way to "tell" laptops they are at an Internet café to make them more suspicious of contact from other computers.

"When you go to an Internet café, you tell your computer you are there and it can put up these defenses. Anti-virus companies can do the same thing through software that stops your computer from being misled and re-directed to someone else," says Aycock.

Why worry about ads? Aycock explains it this way: "Not only are ads annoying but they can also advertise rogue antivirus software that's harmful to your computer, so ads are in some sense the tip of the iceberg."

More information: The paper Typhoid Adware can be found: pages.cpsc.ucalgary.ca/~aycock/papers/eicar10.pdf

Provided by University of Calgary

Citation: Researchers predict new computer security threat for wireless networks: Typhoid adware (w/ Video) (2010, May 21) retrieved 9 April 2024 from https://phys.org/news/2010-05-threat-wireless-networks-typhoid-adware.html