
Warning of webmail wi-fi hijack

Using public wi-fi hotspots has got much riskier as security experts unveil tools that nab login data over the air.

Demonstrated at the Black Hat hacker conference in Las Vegas, the tools make it far easier to steal account details, said Robert Graham of Errata Security.

Identifying files called cookies are stolen in the attack which let hackers pose as their victim.

This gives attackers access to mail messages or the page someone maintains on sites such as MySpace or Facebook.

Hacker gathering

Prior to the demonstration, which involved the live hijacking of a Google mail account (GMail), many sites were thought to be safe because they encrypted the data swapped back and forth when people login.

However, Mr Graham carried out his attack on the unencrypted cookies, tiny text files, many sites use to identify people that regularly return.

The tools created by Mr Graham, called "Hamster" and "Ferret", watch the traffic flowing in and out of public wi-fi hotspots and let attackers grab cookies as they are passed back to people logging in to their webmail or social network account.

Using the cookie an attacker could pose as a victim and enjoy almost the same level of access to an account as its rightful owner.

There were some defences against the attack, said Mr Graham.

Attackers would be unable to change a password and take over an account as most sites ask people to re-enter their old password before letting them make changes.

Also, said Mr Graham, some webmail services, such as GMail, let people encrypt all the data passed back and forth as they deal with their mail.

Mr Graham revealed his findings during a presentation at the four-day Black Hat conference held in Las Vegas. The conference brings together security professionals around the world who swap information about the latest exploits and future vulnerabilities.

He said Errata would make the attack tools publicly available via the company's website for anyone to download.

Also at the conference David Thiel, of security firm iSec Partners, revealed that PC media players have significant vulnerabilities that could be exploited by hi-tech criminals.

The loopholes could be used to attach malicious programs to music or video downloads in order to hijack a PC.

He suggested that popular pages on social networking sites could be subverted by malicious hackers to add the booby-trapped media files.

"The potential for attack is pretty severe," he said.

Mr Thiel said the makers of the media players had been told about the problems and were working on fixes for them.

Story from BBC NEWS:

<http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6929258.stm>

Published: 2007/08/03 10:36:40 GMT

© BBC MMVII