Web certificate fraud bears Iranian fingerprints

March 24 2011

An Iranian man surfs the Internet at a cafe in Tehran on January 2011. Hackers from Iran are suspected of swiping authentication data from a US computer security firm in an attempt to impersonate popular Google or Yahoo! sites.

Hackers from Iran are suspected of swiping authentication data from a US computer security firm in an attempt to impersonate popular Google or Yahoo! sites.

"The incident got close to, but was not quite, an Internet-wide security meltdown," Electronic Frontier Foundation senior staff technologist Peter Eckersley said in a message posted at the group's website.

Hackers using computers with addresses in Iran posed as a European affiliate of New Jersey-based Comodo on March 15 to get digital

certificates allowing the creation of imitation Google, Yahoo!, Microsoft or Skype log-in pages.

"The attacker was well prepared and knew in advance what he was to try to achieve," Comodo said in an online message regarding the attack. "He seemed to have a list of targets that he knew he wanted to obtain certificates for."

The hacker got "SSL certificates," essentially digital credentials, to pose as mail.google.com, google.com, login.yahoo.com, login.skype.com, addons.mozilla.org, global.trustee and login.live.com.

"These fraudulent SSL certificates could be used by an attacker to masquerade as a trusted website," the US Computer Emergency Readiness Team warned.

One of the online identities was tested on an Iranian computer server but the others appeared not to have been used, according to Comodo, which said that it revoked the credentials within hours.

Microsoft, Mozilla, and Google have updated their Web browsing software to prevent being duped into trusting bogus websites using the credentials.

"These certificates may be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against all Web browser users including users of Internet Explorer," Microsoft said in a security advisory.

Whoever was behind the attempt appeared to be out to monitor or intercept email messages or Skype calls.

"This was likely to be a state-driven attack," Comodo said. "The

circumstantial evidence suggests that the attack originated in Iran."

(c) 2011 AFP