PHYS.ORG

Google users in Iran targeted in certificate scam

August 30 2011, by Chris Lefkow

A false Internet security certificate has been used in an apparent attempt to snoop on Google users in Iran, according to the Internet search giant and computer security firms.

A false Internet security certificate has been used in an apparent attempt to snoop on Google users in Iran, according to the Internet search giant and computer security firms.

A Dutch company, DigiNotar, which issues the Internet security credentials known as SSL certificates, said on Tuesday that it had revoked the "fraudulent certificate" in question.

SSL certificates are used to verify to visitors that a particular website is authentic and are issued by DigiNotar and other firms known as Certification Authorities.

Internet users whose browsers are fooled by a false certificate could unwittingly reveal their activity to another party in what is known as a "man-in-the-middle attack."

DigiNotar said it had suffered an "intrusion" into its Certificate Authority infrastructure on July 19 which resulted in the "fraudulent issuance of public key certificate requests for a number of domains, including Google.com."

"At that time, an external security audit concluded that all fraudulently issued certificates were revoked," DigiNotar said. "Recently, it was discovered that at least one fraudulent certificate had not been revoked at the time.

"After being notified by Dutch government organization Govcert, DigiNotar took immediate action and revoked the fraudulent certificate," it said.

Google said in a blog post late on Monday that it had "received reports of attempted SSL man-in-the-middle attacks against Google users, whereby someone tried to get between them and encrypted Google services.

"The people affected were primarily located in Iran," said Heather Adkins, an information security manager at Google.

"The attacker used a fraudulent SSL certificate issued by DigiNotar, a root certificate authority that should not issue certificates for Google," she said.

Adkins said users of the Google Chrome Web browser were protected from the attack "because Chrome was able to detect the fraudulent certificate."

"To help deter unwanted surveillance, we recommend that users, especially those in Iran, keep their Web browsers and operating systems up to date and pay attention to Web browser security warnings," she added.

Microsoft, maker of the Internet Explorer Web browser, said it had removed the DigiNotar certificate from the "Microsoft Certificate Trust List."

Mozilla, maker of the Firefox browser, said it was releasing new desktop and mobile versions of Firefox "that will revoke trust in the DigiNotar root and protect users from this attack."

Computer security firm F-Secure said there was a similar incident in May that was "tied to Iran" and "it's likely the Government of Iran is using these techniques to monitor local dissidents."

F-Secure said an attacker using a false SSL certificate could potentially "impersonate Google -- assuming you can first reroute Internet traffic for google.com to you.

"This is something that can be done by a government or by a rogue ISP (Internet Service Provider)," it said.

F-Secure also said the intent would not be to monitor traffic to search engine google.com.

"This is about the Gmail servers at mail.google.com and Google Docs at docs.google.com and maybe Google+ at plus.google.com," it said.

Citation: Google users in Iran targeted in certificate scam (2011, August 30) retrieved 2 April

2024 from https://phys.org/news/2011-08-google-users-iran-certificate-scam.html