



Home > Data Breaches >

March 23, 2011, 3:23PM

Phony SSL Certificates issued for Google, Yahoo, Skype, Others

by Paul Roberts



Share



Recommend (1)



19 Comments

UPDATED: A major issuer of secure socket layer (SSL) certificates acknowledged on Wednesday that it had issued 9 fraudulent SSL certificates to seven Web domains, including those for Google.com, Yahoo.com and Skype.com following a security compromise at an affiliate firm. The attack originated from an IP address in Iran, according to a statement from Comodo Inc.

Comodo, of Jersey City, New Jersey, said, in a [statement on its Web page](#), that an attacker was able to obtain the user name and password of a Comodo Registration Authority (RA) based in Southern Europe and issue the fraudulent certificates. The company said the hack did not extend to its root keys or intermediate certificate authorities, but did constitute a serious security incident that warranted attention.

SSL Certificates are the Internet equivalent of drivers' licenses, said Paul Turner, the vice president of products and customer solutions at [Venafi](#), an Enterprise Key and Certificate Management firm. The bogus certificates could be used in phishing or man in the middle attacks against organizations that haven't updated their certificate revocation lists, he said. They could also be used to sign applications and plug ins, he said.

Most large organizations might store hundreds- or thousands of unique certificates on Web servers, application servers, mainframe systems and end user workstations. However, organizations typically do a poor job of keeping track of which certificates they use and where they are stored. The Comodo breach will force organizations that might replace one or two certificates in a year to swap out nine certificates in a matter of hours - a painstaking and multi-step process that is often handled manually.

The article above is in an abbreviated form. See full article at:

http://threatpost.com/en_us/blogs/phony-ssl-certificates-issued-google-yahoo-skype-others-032311

Milestone Systems is an authorized reseller of VENAFI software, the proven best way to automate EKCM to avoid attacks like the Comodo breach.

ask@milestonesystems.com

www.milestonesystems.com

866-646-9211

milestone
systems, inc.

