DigiNotar Files for Bankruptcy in Wake of Devastating Hack

- By Kim Zetter
- 09.20.11 |
- 3:05 pm |
- Permalink

- Share on Facebook
  0
-
-
-
-

A Dutch certificate authority that suffered a major hack attack this summer has been unable to recover from the blow and filed for bankruptcy this week.

DigiNotar, which is owned by Illinois-based Vasco Data Security and was the primary provider of digital security certificates for domains owned by the Dutch government, was breached in early June due to lax security.

The breach allowed the intruder to trick DigiNotar's system into issuing him more than 500 fraudulent digital certificates for top internet companies like Google, Mozilla, and Skype. This meant that users who went to a supposedly secure page such as https://google.com were at risk of having a malicious third party who possessed the Google certificate pose as the legitimate site and trick the user into entering his username and password into the impostor site.

The breach resulted in an immediate loss of trust in DigiNotar's integrity as an authority for issuing secure digital certificates, and resulted in swift action from the Dutch government, which pulled its business from the company.

In announcing the bankruptcy filing, DigiNotar's parent company took pains to distance itself from the breach.

"The technological infrastructures of Vasco and DigiNotar remain completely separated, meaning that there is no risk for infection of Vasco's strong authentication business," said T. Kendall Hunt, Vasco's chairman and CEO in a statement. "In addition, we plan to cooperate with the Trustee and the Judge to the fullest extent reasonably practicable to bring the affairs of DigiNotar to an appropriate conclusion for its employees and customers."

DigiNotar is one of numerous firms around the world that generate security certificates for internet entities. The certificates authenticate web pages using the Secure Socket Layer protocol (SSL) so that users can trust that their encrypted communication is going to the correct location. Someone who manages to steal a certificate – such as criminals or rogue government agents – can impersonate a legitimate site to not only steal log-in credentials but also read a user's communications. To do this, an attacker would either need to be on the same network as the victim, in order to intercept traffic going to the legitimate site, or a government-controlled ISP could use the certificate to redirect traffic to a bogus site to spy on users.

According to a third-party audit of the breach, DigiNotar had been hacked in early June, but didn't uncover the breach until mid-July, when it discovered that the intruder had successfully issued himself digital certificates. The audit, conducted by security firm Fox-IT in the Netherlands, revealed that DigiNotar had lacked basic security safeguards, such as strong passwords, anti-virus protection, and up-to-date software patches.

DigiNotar remained mum on the breach until late August, however, when reports began circulating from people in Iran who claimed they were getting browser error messages when they tried to load the Gmail website. Google subsequently confirmed that a fraudulent Google certificate issued to a non-Google entity was operating in the wild, allowing someone to conduct a man-in-the-middle attack to intercept Gmail traffic.

DigiNotar then admitted that someone had breached its network months earlier and had obtained certificates for an undisclosed number of domains. The company insisted that all of the certificates had been revoked — which would have undermined any attempt by someone to use the certificate to impersonate a legitimate site — but somehow missed the Google certificate. Diginotar finally revoked the Google certificate after the search giant disclosed its existence in the wild.

DigiNotar wouldn't identify the other victims at the time it disclosed the breach and was roundly criticized for the way it handled the issue. Browser makers Google, Mozilla and Microsoft subsequently announced that they would permanently block all digital certificates issued by DigiNotar, suggesting a complete loss of trust in the integrity of its service. The Minister of the Interior for the Netherlands also announced that the government could no longer guarantee the security of its websites and urged the public not to log into them until new certificates could be obtained from other issuing authorities.

It was only after Fox-IT released its audit report that an accounting of the number of certificates that had been issued to the intruder could be made. But Fox-It acknowledged in its report that a final list of sites affected could not be determined, since the intruder had managed to erase logs that might have provided additional information about his activity.

A hacker who previously claimed credit for breaching Comodo, another certificate authority, earlier this year claimed responsibility for the DigiNotar breach. The hacker, who in the past has identified himself as a 21-year-old Iranian student, claimed he got root access to DigiNotar after obtaining an administrator's username (Production/Administrator) and password (Pr0d@dm1n). He also claimed to have breached four other certificate authorities, but did not name them.

The hacker claimed the attack was political retaliation for what he considered was complicity on the part of the Dutch government in the Serbian massacre of 8,000 Muslims in July 1995 during the Bosnian War.

The hacker hinted that he provided the fraudulent Google certificate and others to the Iranian government. If this is the case, the government could have deployed the certificate on major ISPs in Iran in order to spy on political dissidents who used Gmail.

The hacker claimed the attack was political retaliation for what he considered was complicity on the part of the Dutch government in the Serbian massacre of 8,000 Muslims in July 1995 during the Bosnian War.

The hacker hinted that he provided the fraudulent Google certificate and others to the Iranian government. If this is the case, the government could have deployed the certificate on major ISPs in Iran in order to spy on political dissidents who used Gmail.