Second firm warns of concern after Dutch hack

September 7 2011, By TOBY STERLING , Associated Press

Exterior view of the building housing Internet security firm DigiNotar in Beverwijk, north-western Netherlands Tuesday Sept. 6, 2001. Dutch prosecutors say they are investigating DigiNotar for possible criminal negligence after it was slow to disclose a hacking incident that compromised dozens of websites and likely helped the Iranian government spy on dissidents for a month. DigiNotar, a subsidiary of Chicago-based Vasco Inc., did not return phone calls seeking comment. Spokesman Ernst Koeman of the Netherlands' national prosecutor's office said Tuesday the investigation is in a preliminary phase. (AP Photo/Peter Dejong)

A company that sells certificates guaranteeing the security of websites, GlobalSign, said Tuesday it is temporarily halting the issuance of new certificates over concerns it may have been targeted by hackers.

GlobalSign, the Belgium-based subsidiary of Japan's GMO Internet Inc., is one of the oldest such companies globally, and large, but much smaller than industry giants VeriSign and GoDaddy.

It said in a statement it does not know whether it has actually been hacked, but is taking threats by an anonymous hacker seriously in the wake of an attack on a smaller Dutch firm, DigiNotar, that came to light last week.

The DigiNotar attack is believed to have allowed the Iranian government to spy on thousands of Iranian citizens' communications with Google email during the month of August.

Fallout from the Dutch hack continued Tuesday as the Dutch government, which used DigiNotar to authenticate many of its sites, continued to seek replacements.

Meanwhile the Netherlands' national prosecutors said they were investigating DigiNotar, a subsidiary of Chicago-based Vasco Inc., for possible criminal negligence.

The company did not return phone calls seeking comment.

A Dutch government review of the incident conducted by external information technology experts found that DigiNotar - whose business is ensuring digital security - had itself used weak passwords, failed to update software on its public servers and had no antivirus protection on its internal servers.

The company first acknowledged it had been hacked on Aug. 30, a day after Google publicly stated that fake and unauthorized DigiNotar certificates for Google sites were circulating in Iran. Google marked the company's certificates as dubious, and other web browser makers followed suit.

Only then did DigiNotar acknowledge being hacked on July 19, saying that hackers had issued fake certificates for "a number" of domains. The company said it believed it had withdrawn them all, but missed Google.

On Sept. 3, the Dutch government seized control of DigiNotar's operations, saying certificates the company had issued to guarantee the safety of numerous Dutch government websites could also no longer be relied on.

The external review by Fox-IT found that the company was actually hacked on June 17th and that hackers had issued 531 bogus certificates for 344 domains in all, including most major Internet communications companies.

The fake Google certificates had been used by 300,000 IP addresses by then, more than 99 percent of them in Iran.

Fox-IT and other experts have concluded the hackers were helping the Iranian government spy on citizens who thought they were accessing Google email securely due to the bogus DigiNotar seal of approval.

"We are definitely going to look at...whether this is culpable negligence by the company that they didn't report this," Interior Minister Piet Hein Donner said at a news conference late Monday.

The government also is investigating who was behind the hack, though that may be difficult to verify without help from Tehran.

An unknown hacker who claimed responsibility for a similar breach of U.S.-based certificate issuer Comodo Inc. in March, has also claimed responsibility for the DigiNotar hack.

In a posting on Pastebin.com under the handle "ComodoHacker" on

Monday, he or she offered a user name and password for an administrator's account at DigiNotar as evidence.

The post also boasted of having hacked four other "high profile" certificate providers, including GlobalSign.

"GlobalSign takes this claim very seriously and is currently investigating," the company said in a statement.

"ComodoHacker" has used phrases in the Farsi language spoken in Iran in previous posts to Pastebin - including a phrase that also was found by Fox-IT in a message left on DigiNotar's servers. Monday's post cited anti-Dutch political motivations for the attacks.

Donner said that in the wake of the incident the Dutch government is considering legislation that would make it mandatory for companies to disclose computer hacks and data leaks.

Citation: Second firm warns of concern after Dutch hack (2011, September 7) retrieved 26 April 2024 from https://phys.org/news/2011-09-firm-dutch-hack.html