MUST READ WINDOWS 10 AT SIX MONTHS: READY FOR PRIMETIME?

Just how many websites are vulnerable because of SHA-1?

Naughty certificate authorities are breaching agreed timelines for phasing out digital certificates signed with the insecure SHA-1 hashing algorithm.

By Liam Tung | October 20, 2015 -- 11:11 GMT (04:11 PDT) | Topic: Security

Some certificate authorities are still issuing digital certificates signed with the SHA-1 hashing algorithm, despite recent research showing that the cost of undermining it is not beyond criminals' budgets.

Browser makers Google, Microsoft, and Mozilla have announced plans to stop accepting SHA-1 SSL certificates by 2017.

But researchers recently called for this deadline to be brought forward, after estimating the cost of causing a SHA-1 collision is much cheaper than initially thought - and definitely within reach of cybercriminal budgets.

"Concretely, we estimate the SHA-1 collision cost today of between $75,000 and $120,000, renting Amazon EC2 cloud computing over a few months," researchers Marc Stevens, Pierre Karpman, and Thomas Peyrin noted earlier this month.

They based their estimate on "freestart collision" SHA-1 experiments using a 64-GPU Kraken cluster, which consisted of 16 nodes made from commodity hardware including four GTX-970 GPUs, one Haswell i5-4460 processor, and 16GB of RAM.

Cryptographer Bruce Schneier previously projected the SHA-1 collision cost to be about $173,000 by 2018.

Despite consensus that time is nearly up for SHA-1, an SSL survey by security firm Netcraft has found that almost one million SSL certificates for websites are still signed with SHA-1.

"Nearly a million SSL certificates found in Netcraft's October SSL Survey were signed with the potentially vulnerable SHA-1 hashing algorithm, and some certificate authorities are continuing to issue more," Netcraft's Paul Mutton said.

READ THIS

Is cybercrime more of a threat than terrorism?

Intelligence officials believe so, saying that cyberattackers are the main threat against the United States in the modern era.

Read More

Mutton noted that certificate authorities are meant to be forbidden from 2016 from issuing new subscriber certificates or subordinate certificates that use the SHA-1 algorithm.

Despite this deadline and concerns over SHA-1's security, this year alone certificate authorities have issued 120,000 SHA-1 certificates.

One of the sources of new SHA-1 certificates is large enterprise customers, according to Mutton.

"Symantec proposed a motion, endorsed by Entrust, Microsoft, and Trend Micro, to allow the issuance of SHA-1 signed certificates throughout 2016," he noted. The point was to support "a very small number of very large enterprise customers" who could not migrate to the more secure SHA-2 by deadline.

However, Symantec dropped the motion after the researchers revealed their cost estimates for causing a SHA-1 collision.

To make things worse, some SHA-1 certificates are valid well beyond the 2017 timeframe. According to Mutton, 3,900 SHA-1 certificates exceed this date.

Read more about SHA-1

- Putting the cracking of SHA-1 in perspective
- Google accelerates end of SHA-1 support; certificate authorities nervous
- Is Chrome flagging your bank's website for weak security?