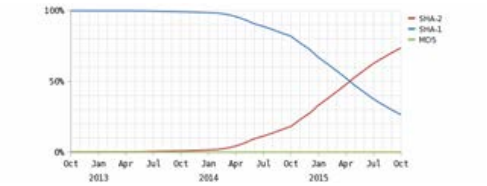
Tim Ring

October 20, 2015

Nearly 1m sites at risk because they use 'insecure' SHA-1 encryption

Close to 1 million websites are at risk from fraudsters because they continue to place their trust in security certificates using the vulnerable SHA-1 hashing algorithm.

Bath-based internet services provider Netcraft has warned that large Government, banking and corporate SHA-1 certified sites are most threatened, after new research showed it is up to 10 times cheaper than previously thought to crack their crypto and launch fake sites impersonating them.



Nearly 1m sites at risk because they use 'insecure' SHA-1 encryption

Netcraft security researcher Paul Mutton said In a 19 October blog that SHA-1 based certificates are about to be banned – the CA/Browser Forum governing body has ruled no new such certificates can be issued after the start of 2016, and it already bars any existing certificates that are valid beyond the end of 2017.

Meanwhile, NIST also only approves of new certificates using the stronger SHA-2 and SHA-3 cryptography.

Despite that, new figures from Netcraft show nearly a million sites still use SHA-1 security. More than 120,000 such certificates have been issued by CAs (Certificate Authorities) this year and 3,900 of these have an expiry date beyond the permitted 2017 deadline.

Netcraft said one corporate still using SHA-1 based SSL security is Deloitte Austria. Its certificate from A-Trust was issued in February and is valid until 2020, well beyond the permitted time limit.

The vulnerability of such sites is being exposed by Google's Chrome browser, which flags any existing SHA-1 certificates due to expire during 2016 as weak, and brands any certificates valid beyond the start of 2017 as “affirmatively insecure”.

And Paul Mutton said the risk to these sites is now much greater, after the latest so-called 'SHAppening' research, published two weeks ago, showed that well-funded attackers could mimic SHA-1 based sites for a cost of about US$ 75,000 to US$ 120,000 (£49,000 to 78,000) – up to 10 times less than previously thought.

As a result, Netcraft is warning that industry plans to move away from SHA-1 by 2017 may not be fast enough.

Mutton told *SCMagazineUK.com*: "The SHAppening research shows the cost of finding a hash collision is much lower than previously thought. Finding one of those hash collisions means that you can potentially imitate someone else's secure website. So it means there is a much more pressing need for people to migrate from SHA-1 to SHA-2.

"If you're using these certificates there is a chance that someone with enough money and enough impetus could imitate your website. In practice Joe Bloggs is unlikely to be a target if it's going to cost US$ 75k (apx £50K) to attack you but Government websites, banks and so on, if they're still using SHA-1 they're probably the most likely ones to be attacked by man-in-the middle attackers. Sites that are still using SHA-1 certificates ought to think about moving sooner rather than later."

Mutton said Google Chrome's branding of sites with SHA-1 certificates valid beyond 2017 as insecure "is going to drive certificate authorities into stopping that practice".

Commenting on Netcraft's findings, cyber-security expert David Kennerley, threat research manager at Webroot, supported its call for action.

He told *SCMagazineUK.com* via email: "There is no good reason for digital certificates to still be signed with SHA-1 when there is a well-documented and available alternative, SHA-2. Companies not upgrading to SHA-2 are publicly advertising their poor attitude towards security. In simple terms they are stating that the security of their website, its visitors and its transactions is not their highest priority.

"Certificate authorities also need to take responsibility – this deadline shouldn't be taking anyone by surprise as it's been well-reported. Chrome is leading the way as a browser, taking a stand and warning its users of possible issues. The worry is that users are becoming desensitised to such warnings and are taking more risks. This is the perfect recipe for phishing attacks and fake websites!"

Kennerley added: "The digital world as we know it is wholly reliant on a fully functional and well-maintained public key infrastructure. As the cost of computing power decreases we will continue to see previously trusted algorithms in need of replacement on security grounds. We should not be making it easy for anyone to acquire our private communications."

Kevin Bocek, VP of security strategy at Venafi, told *SCMagazineUK.com* via email: "For the last 10 years, the security community has been urging organisations to move away from SHA-1. Now that an attack is feasible for US$ 75k, it's urgent that businesses realise the need to replace SHA-1 certificates now, not next year. With over a million SHA-1 certificates still out there, we could get a glimpse of what a potential 'crypto-apocalypse' could look like: we wouldn't know if we could trust any certificates, and the ability to replace them would take some time.

"Every organisation should be scanning their networks, clouds and devices looking for SHA-1 and other certificate risks, including anything not in policy, and replacing them. To do this, organisations will need to know who owns the certificates, who administers the systems involved, and be able to report on the progress of remediation until complete."

Netcraft's latest warning on insecure SSL website certificates follows its revelation last week that hundreds of fraudulent sites purporting to be the official domains of PayPal, Halifax Bank and others managed to get security clearance from certificate authorities including CloudFlare, Symantec and GoDaddy.

We asked Deloitte to comment on Netcraft's findings but it had not responded by time of writing.