RSA Conference starts soon
RSAConference
San Francisco | February 29–March 4 |
STRATEGY | INSIGHT | TECHNOLOGY

13 OCT 2015 NEWS

# Web Owners Urged to Upgrade From Insecure SHA-1 Algorithm

Phil Muncaster
UK / EMEA News Reporter , Infosecurity Magazine
Email Phil
Follow @philmuncaster

Security experts are urging website owners to ensure their SSL certificates are signed with the SHA-2 algorithm, after discovering a new way to crack the old SHA-1 version.

Advances in computing technology have made it increasingly cost effective for attackers to target hashing algorithm SHA-1, which is used to sign around a third of the SSL certs used to secure websites.

That's why web browsers will no longer accept these certificates after 1 January 2017.

However, a new team of researchers has estimated it would cost between $75,000 and $120,000 to rent public cloud services to launch such an attack – still expensive but within the reach of major cybercrime gangs.

There are also mutterings within the Certificate Authority industry that the January 2017 deadline might be extended.

Now researchers from Singapore's Nanyang Technological University (NTU), Centrum Wiskunde and Informatica in the Netherlands and France's NTU and Inria have described a way to simplify an "identical-prefix" attack on SHA-1.

It would not allow attackers to generate fake SSL certificates, but the research should be seen as yet another sign that the legacy hashing algorithm has had its day, according to IDG.

Kevin Bocek, vice president of security strategy & threat intelligence at Venafi, argued that the widespread use of a flawed algorithm is sending a clear message to cybercriminals: "feel free to mount more web attacks on us because we're too lazy to upgrade to SHA-2."

He claimed Venafi found over 1.5 million certificates using SHA-1 which were issued after NIST had deprecated its usage.

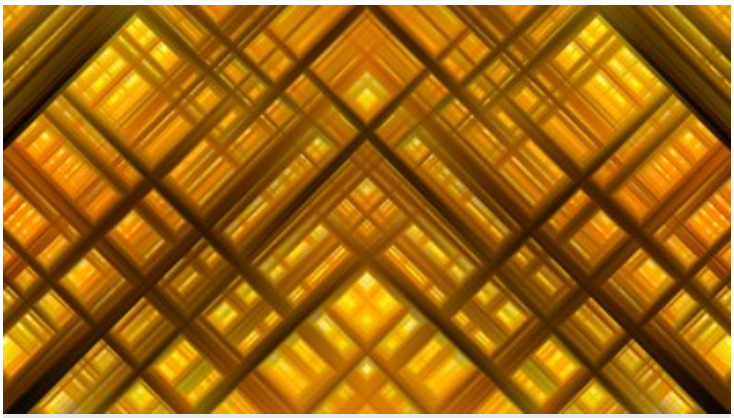
"If we don't start taking the security of digital certificates and cryptographic keys seriously, we'll continue living in a world without trust – a world without an immune system – and a world where a cryptoapocalypse will inevitably happen," he argued.

"We urge the industry to consider shifting this deadline up and enterprises should not wait any longer to migrate to SHA-2."

IT security teams should locate SHA-1 certificates immediately, automate the transition process and report on their progress before the 2017 deadline, Bocek added.

Web2PDF
converted by Web2PDFConvert.com


## Why Not Watch?



5 FEB 2015

Encryption Under Attack: Government vs Privacy

21 JAN 2016

Don't Be Blind On Visibility


7 JAN 2016

The 'Dark' Web Inside Your Enterprise – Shining a Light on the Hazards of Encrypted Traffic

2 APR 2015

Browsers, Certificates and Trust: What's Changing and What You Need to Know

## Related to This Story

UK Online Banking Log-On Pages Deeply Vulnerable

Google Demands Changes After More Rogue Symantec SSL Certs Found

Critcial BERserk Flaw Opens Door to SSL Spoofing and MiTM Attacks

Mobile App Research Shows Major Flaws Persist

Google Preps New Service after Global Email Encryption Warning

Web2PDF
converted by Web2PDFConvert.com

# What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1. 28 JAN 2016 NEWS
   Panda Security Spotted Over 80 Million New Malware Samples in 2015
2. 28 JAN 2016 NEWS
   Employee Retention is Critical to Solving the Security Skills Shortage
3. 28 JAN 2016 NEWS
   Large-Scale Hacks Cause 98% of Leaked Healthcare Records
4. 28 JAN 2016 NEWS
   DDoS Attacks Hit Record 500 Gbps in 2015
5. 20 FEB 2013 MAGAZINE FEATURE
   The Dark Side of Cryptography: Kleptography in Black-Box Implementations
6. 28 JAN 2016 NEWS
   Wendy's Investigates Possible Data Breach







**Our website uses cookies**

Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By browsing Infosecurity Magazine, you agree to our use of cookies.

Okay, I understand | Learn more

Copyright © 2016 Reed Exhibitions Ltd.
Terms and Conditions
Privacy Policy
Use of Cookies
Sitemap

Reed Exhibitions

Web2PDF
converted by Web2PDFConvert.com