

Złamanie SHA-1 tańsze niż sędzono

10 października 2015

Szeroko używana funkcja skrótu SHA-1 ma odejść do lamusa w 2017 roku. Jednak niewykluczone, że stanie się to wcześniej, gdyż udowodniono, iż atak na tę funkcję jest tańszy, niż dotychczas sędzono. Grupa ekspertów wykazała, że wystarczy wydać 75 000 USD na wynajęcie odpowiednich mocy obliczeniowych w chmurze, by poznać treści zabezpieczone za pomocą SHA-1. Gdy w 2012 roku zdecydowano, że SHA-1 nie będzie używana po roku 2017 szacowano, iż wówczas złamanie skrótu będzie kosztowało 173 000 dolarów. Teraz, gdy dowiedziono, iż jest o 100 000 USD tańsze, stało się jasne, że o atak na tę funkcję mogą pokusić się dobrze wyposażone grupy cyberprzestępców. To z kolei może skłonić przemysł do szybszego porzucenia SHA-1.

„Nie jest to coś, czego się nie spodziewaliśmy” – mówi znany ekspert Bruce Schneier. „Producenci wszystkich głównych przeglądarek przestaną do roku 2017 akceptować SHA-1, a Microsoft uczyni to też w swoich innych produktach. Nową wiadomością jest tu jedynie fakt, że nasze wcześniejsze oceny kosztów ataku były błędne” – stwierdza.

Ataku dokonali Marc Stevens z holenderskiego Centrum Wiskunde & Informatica oraz Pierre Karpman i Thomas Peyrin z singapurskiego Uniwersytetu Technologicznego Nanyang. Do ataku wykorzystano klaster Kraken korzystający z 64 kart graficznych GTX 970 Nvidii. Atak trwał 10 dni, a w jego czasie udało się złamać pełne 80 cykli SHA.

Autorstwo: Mariusz Błoński

Na podstawie: TheRegister.co.uk

Źródło: KopalniaWiedzy.pl