COMPUTERWORLD

Złamanie SHA-1 w chmurze kosztuje 75 tys. USD

Wyniki badań udowadniają, że SHA-1 nie zapewnia oczekiwanego poziomu bezpieczeństwa i nie powinien być stosowany, gdyż koszt jego złamania jest bardzo niski. Prawdopodobnie już w lipcu przyszłego roku certyfikaty podpisane z użyciem algorytmu SHA-1 nie będą uznawane przez przeglądarkę Firefox.

Marcin Marciniak
25.10.2015, godz. 23:31

Kryptolodzy niejednokrotnie wspominali o tym, że algorytm SHA-1 nie chroni już przed atakami klasy militarnej. Kilka tygodni temu potwierdzili to Thomas Peyrin z Politechniki w Nanyang (Nanyang Technological University) w Singapurze, Marc Stevens z holenderskigo Centrum Wiskunde and Informatica, a także Pierre Karpman, który współpracuje z NTU i Inria we Francji.

Opublikowany przez nich dokument opisuje nowy atak, który umożliwia złamanie SHA-1. Badacze szacują, że złamanie pełnych 80 rund SHA-1 przy użyciu komercyjnie dostępnych zasobów obliczeniowych w chmurze może kosztować pomiędzy 75 tys. a 120 tys. USD. Jest to poziom cen akceptowalny

dla wielu grup cyberprzestępców, zainteresowanych wykorzystaniem luki w bezpieczeństwie SHA-1 na przykład do kreowania fałszywych certyfikatów. W wywiadzie, którego udzielił Thomas Peyrin dla IDG News Service, powiedział: *„zalecamy branży, by nie igrała z ogniem i przyspieszyła migrację do SHA-2 i SHA-3 zanim takie ataki staną się realne”*.

Zobacz również:

- **Badanie bezpieczeństwa sieci**
- **Mozilla Foundation ma się dobrze**

Ludzie z branży zdają się słuchać porad i wyciągać wnioski – działania w zakresie pomocy w migracji rozpoczęła firma Symantec, do której dołączyły Entrust, Microsoft i Trend Micro. Pomogą oni *„bardzo małej grupie wielkich klientów korporacyjnych”* w migracji do certyfikatów z użyciem SHA-2. Proces migracji powinien zakończyć się jeszcze w tym roku.

Let's Encrypt startuje w grudniu

Webmasterzy, którzy obawiają się wysokich kosztów wymiany certyfikatów, będą mieć niebawem darmową alternatywę. Organizacja non-profit Let's Encrypt poinformowała, że jej certyfikat root został podpisany przez IdenTrust, a zatem będzie uznawany za zaufany we wszystkich najważniejszych przeglądarkach. Certyfikaty wydawane przez Let's Encrypt powinny być dostępne już w grudniu bieżącego roku.

Milion słabych certyfikatów

Jak podaje Netcraft, ponad milion certyfikatów nadal korzysta ze słabego algorytmu, 120 tysięcy z nich było wydanych w 2015 roku, a 3900 ma termin ważności przypadający na czerwiec 2017 lub później. Według statystyk SSL Pulse, aż 24% spośród 143 tysięcy stron HTTPS klasyfikowanych pod względem największego ruchu odbywa się przy użyciu certyfikatów wykorzystujących ten niebezpieczny algorytm.

Czy wszyscy twórcy przeglądarek zablokują SHA-1?

W świetle obecnych postępów nad łamaniem funkcji kryptograficznej SHA-1 Mozilla rozważa zablokowanie w przeglądarce Firefox uznawania cyfrowych certyfikatów podpisanych z użyciem tego algorytmu. Na forum CA/Browser grupa ekspertów tworzących zasady i zalecenia wskazała, że nowe certyfikaty podpisane z użyciem funkcji SHA-1 nie powinny być wystawiane po 1 stycznia 2016 roku, a przestaną być uznawane w przeglądarce rok później. We wtorek Mozilla poinformowała, że wycofanie obsługi tego przestarzałego algorytmu powinno nastąpić wcześniej – 1 czerwca przyszłego roku. Wskazówką do podjęcia tej decyzji były wyniki eksperymentów nad łamaniem SHA-1.

Konkurencyjna przeglądarka Google Chrome już wyświetla inny symbol połączenia SSL, jeśli certyfikat danej strony używa przestarzałego algorytmu. Mozilla zamierza pójść znacznie dalej, by zachęcić właścicieli stron do migracji z SHA-1 na rzecz nowszych SHA-2 lub SHA-3.

Mozilla Foundation ma się dobrze

Mozilla Foundation donosi, że jej przychody wzrosły w 2014 finansowym roku o 5%. Fundacja uzyskała tak dobry wynik głównie dzięki umowie z firmą Google. Zapłaciła ona jej sporo pieniędzy za to, że jej rozwiązanie było wskazywane przez przeglądarkę Firefox jako domyślna wyszukiwarka.

Janusz Chustecki
01.12.2015, godz. 18:58

Jak można przeczytać w raporcie finansowym opublikowanym przez Mozillę Foundation, jej przychody zamknęły się w 2014 r. kwotą 330 mln USD (rok wcześniej było to 314 mln USD), z czego 291 mln USD było pochodną umów przewidujących, że Firefox będzie wskazywać domyślnie określoną wyszukiwarkę. Analitycy szacują, że Google zapłacił fundacji Mozilla w latach 2012, 2013 i 2014 co najmniej ok. 800 mln USD.

Pod koniec 2014 roku fundacja Mozilla rozwiązała umowę z firmą Google i podjęła współpracę z innym dostawcą oprogramowania przeszukującego Internet – z Yahoo. To właśnie wyszukiwarka Yahhoo jest wskazywana przez amerykańską i kanadyjską edycję przeglądarki Firefox jako domyślna. W Europie Firefox pozostał dalej wierny wyszukiwarce Google. Mozilla Fondation szuka obecnie zysków na innych kontynentach i współpracuje w Chinach z firmą Baidu, a w Rosji z firmą Yandex.

Mozilla postanowiła niedawno pożegnać się z wtyczkami NPAPI i poinformowała, że do końca 2015 roku roku wycofa z obiegu i przestanie budować oraz wspierać wszystkie wtyczki obsługujące przeglądarkę Firefox, które zostały zbudowane przy użyciu przestarzałej już technologii NPAPI

(Netscape Plugin Application Programming Interface). Pisaliśmy o tym niedawno tutaj. Warto przypomnieć, że Google podjął taką decyzję wcześniej i przestał budować takie wtyczki - które obsługiwały jego przeglądarki Google Chrome i Chromium - w 2014 roku.

Jak podaje firma analityczna Net Applications, do przeglądarki Firefox należy obecnie 11,5% tego rynku (najmniej od sierpnia 2006 r.). Jeśli tendencja taka utrzyma się dalej można się spodziewać, że w kwietniu przyszłego roku może to być już poniżej 10%. Liderem na tym rynku będzie wtedy przeglądarka Chrome z udziałem rzędu 35%.

Chrome na Androidzie blokuje malware i skanuje przeglądane strony

Przeglądarka mobilna od Google'a będzie dbała o bezpieczeństwo użytkowników. Twórcy Chrome'a w wersji do Androida dodali do aplikacji mechanizm wykrywania złośliwego oprogramowania znany z desktopowego wydania przeglądarki.

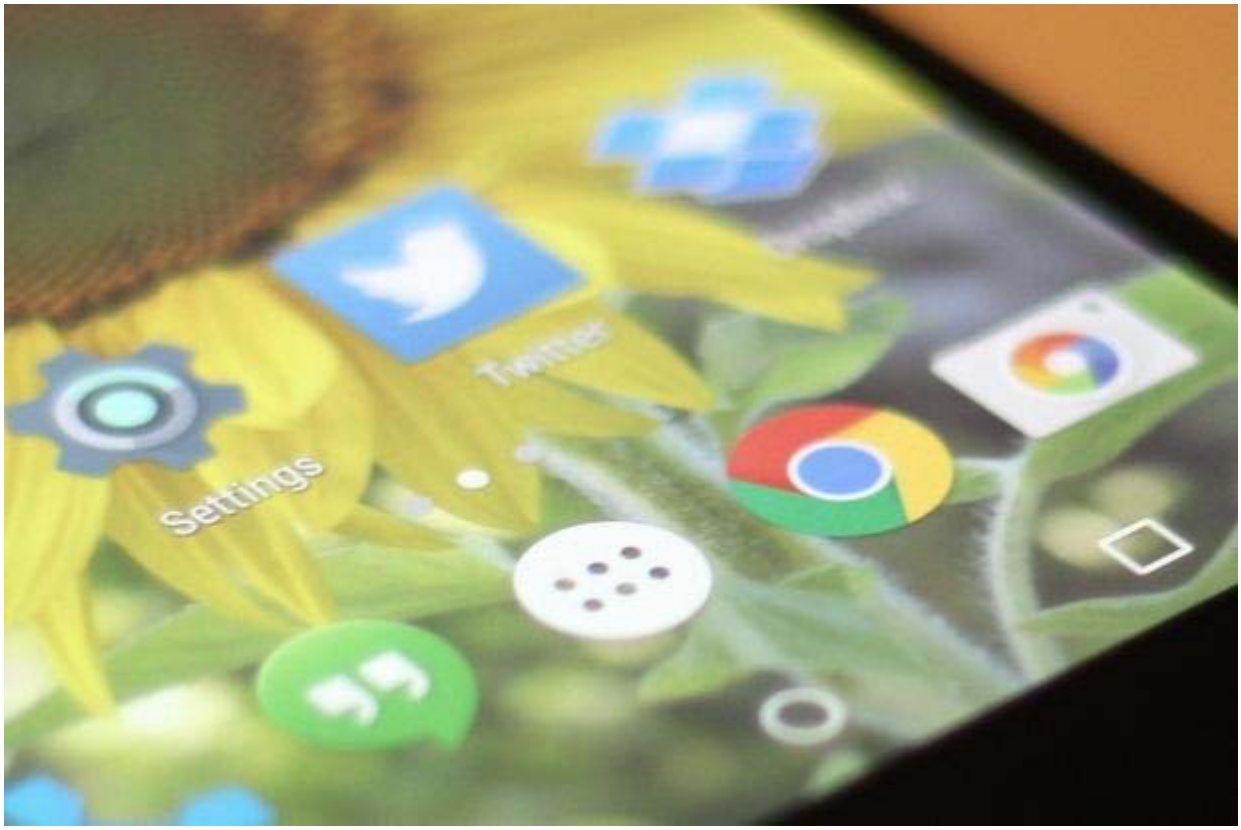
Piotr Grabiec
09.12.2015, godz. 13:10

Użytkownicy Chrome'a na komputerach wchodząc na potencjalnie niebezpieczną stronę internetową są informowani o zagrożeniu. W takiej sytuacji wyświetlana jest czerwona strona z komunikatem o wykrytych problemach i podejrzeniu możliwości pogrania z danej strony złośliwego kodu.

Od teraz dzięki włączeniu w Chrome do Androida funkcji Safe Browsing podobne komunikaty będą się pojawiać również na urządzeniach mobilnych. Dzięki temu użytkownicy mogą w porę się zorientować, że strona na którą się udają może wykradać ich dane lub instalować w ich urządzeniu malware.

Dzięki integracji Safe Browsking rozwiązania z Google Play Services z mechanizmu opracowanego

przez Google'a będą mogły w przyszłości korzystać również inne aplikacje w tym programy dostępne w Google Play. Chrome to pierwszy program, który to wykorzystuje, ale mają pojawić się kolejne.



Mobilny Chrome doczekał się nowej funkcji

Safe Browsing w Androidzie z pewnością przyda się wielu użytkownikom. Chrome do Androida nie obsługuje wtyczek dostępnych w desktopowej wersji przeglądarki, więc nie da się wgrać rozszerzenia pozwalającego wyczyszczenie odwiedzanych stron ze zbędnych elementów.

Google przyznało, że wprowadzenie nowej funkcji wiązało się z kilkoma wyzwaniami. Jednym z nich były małe paczki danych - zwłaszcza wśród użytkowników z tych biedniejszych krajów. Google musiało znaleźć kompromis i wybrać pomiędzy większą ilością informacji na temat stron a wydajnością przeglądarki.

źródło: googleonlinesecurity.blogspot.ro