Powrót Comodohackera? Irańczyk bierze odpowiedzialność za atak na holenderskie CA DigiNotar

Autor: vi.curry | Tagi: atak, Certyfikaty, Comodo, DigiNotar, Hacked!, Iran, włamania

Wszystko wskazuje na to, że za wygenerowaniem 500+ fałszywych certyfikatów w DigiNotar stoi Irańczyk, którego znamy z marcowych ataków na CA Comodo.

Kolejne ofiary: GlobalSign i Google

Comodohacker znany z marcowych ataków na CA Comodo oświadczył, że to on stoi za atakiem na DigiNotar. Jako dowód podał hasło, z którego korzystali Holendrzy: Pr0d@dm1n — prawda, że kreatywne, jak na rządowe CA? :-)

Dodatkowo, Irańczyk twierdzi, że pod kontrolą ma jeszcze kilka innych CA, dzięki którym może generować fałszywe certyfikaty. Jak na razie ujawnił nazwę tylko jedno z nich — **GlobalSign**, a jako dowód, że dalej może fałszować sygnatury, udostępnił calc.exe podpisany kluczem prywatnym wygenerowanym dla **Google**.

Polityka, polityka...

Oświadczenie Comodohackera jak zwykle podszyte jest polityką. Atak na holenderskie CA miał być zemstą za masakrę w Srebrenicy, o którą Irańczyk oskarża Holendrów. Można jednak odnieść wrażenie, że najpierw nastąpił atak, a dopiero potem dopasowany został "powód" pasujący do ofiary. Comodohacker obiecuje niebawem opisać jak przełamał zabezpieczenia holenderskiego CA, dowcipnie pstrykając w nos Anonimowych i LuzSec, twierdząc, że taki opis będzie dla nich dobrą lekcją.

DigiNotar, kolejne zhackowane przez Comodohackera CA

Tymczasem Fox-IT, firma wynajęta do przeprowadzenia audytu w DigiNotar opublikowała swój raport, a w nim punktuje liczne przewinienia CA związane z bezpieczeństwem teleinformatycznym (wszystkie Windowsy w tej samej domenie, brak antywirusów, brak patchy, dostęp do serwerów z vlanu, pomimo umieszczenia ich w "tempeście"). Może się więc okazać, że "wyczyn" Comodohackera nie wymagał super umiejętności, zwłaszcza, że Fox-IT twierdzi, iż atakujący korzystał z populanrnego "hacktoola" Caina i Abla (który nie został wykryty)...

Na koniec garść innych, ciekawych cytatów z oświadczenia Comodohackera to:

> Nie róbcie ze mnie armii. Działam sam.
> Ten atak był bardziej skomplikowany niż Stuxnet. Mam więcej 0day'ów, trojanów oraz certyfikatów podpisujących kod.
> Mam możliwość aktualizowania Windowsów. Zreversowałem protokół aktualizacji Microsoftu.

Czyżbyśmy obserwowali początek końca PKI?