Hakerzy wykradli certyfikaty bezpieczeństwa

25 marca 2011

15 marca społeczność internetowa otrzymała potężny cios. Haker, którego ślady prowadzą do Iranu, wykradł certyfikaty SSL kilku bardziej popularnych serwisów internetowych, do których należą między innymi strony logowania poczty Google, Microsoftu i Yahoo. Haker złamał zabezpieczenia Comodo Group, które specjalizuje się w wystawianiu certyfikatów i w wyniku ataku posiada możliwość podszycia się pod sześć domen: mail.google.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org oraz login.live.com.

Sytuacja jest o tyle groźna, że osoba która dokonała ataku jest w stanie uruchomić podróbki stron, które będą przez przeglądarki widziane jako oryginały. Haker ma możliwość przekierować na swoją maszynę transfer przeznaczony do sieci Skype, Google, czy Yahoo. Działanie takie może mieć miejsce na lokalnej sieci Wi-Fi, ale także pozwala na globalne przejęcie ruchu w sieci. Kiedy już mu się to uda, atakujący może przejąć login i hasło ofiary lub zacząć podglądać sesję użytkownika.

Prezes Comodo, Melih Abdulhayoglu, nazywa włamanie cybernetyczną wersją ataków terrorystycznych na World Trade Center i dodaje, że haker był świetnie przygotowany do włamania. W momencie kiedy udało mu się zalogować do systemu, miał już gotową listę rzeczy, które natychmiast zaczął ściągać. Co więcej, do listy zaufanych certyfikatów dodał swój własny, prowadzący do jego domeny, który nazwał „Globalne Zaufanie”. Abdulhayoglu zaznacza, że włamanie nosi wszystkie znamiona ataku sponsorowanego przez przez kraj lub przedsiębiorstwo. Prezes Comodo tłumaczy to w taki sposób: „Jeśli spojrzy się na skradzione domeny, widać, że każda z nich ma związek z komunikacją. Certyfikaty same w sobie są praktycznie bezużyteczne, jeżeli nie ma się dostępu do

infrastruktury DNS, a jedynie kraje i duże firmy mają dostęp do takiej infrastruktury.”

Mimo że prezes zaznacza, że atak mógł pochodzić skądkolwiek, to został on przeprowadzony przez irańskie serwery proxy, co czyni wg. Abdulhayoglu z irańskiego reżimu oczywistego podejrzanego. Próby testowania skradzionego certyfikatu Yahoo na irańskim IP zdają się potwierdzać te podejrzenia.

Mozilla, Google i Microsoft wydały poprawki, które odrzucają skradzione certyfikaty, więc pobranie najnowszej wersji przeglądarki i jej aktualizacja jest bardzo wskazana jeżeli ktoś nie chce, aby jego konta wpadły w niepowołane ręce.

Opracowanie dla „Wolnych Mediów”: lltr
Na podstawie: www.wired.com