Jak furtkę dostępu NSA wbudowano w system Windows

18 czerwca 2013

Nieostrożny błąd programistów Microsoft spowodował ujawnienie istnienia specjalnych kodów dostępu przygotowanych przez amerykańską Agencję Bezpieczeństwa Narodowego, jakie zostały potajemnie wbudowane w Windows. System dostępu NSA jest wbudowany w każdą wersję systemu operacyjnego Windows, jakich się obecnie używa, z wyjątkiem wczesnych wersji Windows 95 (i jego poprzedników).

Odkrycie to jest zbliżone do informacji z początku tego roku, że inny gigant oprogramowania, Lotus, wbudował dla NSA podobną furtkę „pomocną w zdobyciu informacji" do swojego systemu Notes, oraz że funkcje zabezpieczeń w innych systemach oprogramowania zostały celowo „okaleczone".

Pierwsze odkrycie nowego dostępu NSA do systemu dokonane zostało dwa lata temu przez brytyjskiego badacza dr Nicko van Someren. Ale po kilku tygodniach, to samo potwierdził inny naukowiec. Przy czym znalazł dowody łączące z NSA.

Specjaliści od bezpieczeństwa komputerowego od dwóch lat byli w pełni świadomi, że nietypowe elementy są zawarte wewnątrz standardowego oprogramowania Windows "driver", stosowanych do funkcji zabezpieczeń i szyfrowania. Driver pod nazwą ADVAPI.DLL, umożliwia i reguluje szereg funkcji bezpieczeństwa. Jeśli używasz systemu Windows, znajdziesz go w C:\Windows\system directory.

ADVAPI.DLL ściśle współpracuje z programem Microsoft Internet Explorer, ale uruchomi tylko funkcje kryptograficzne, jakie rząd USA pozwala Microsoftowi eksportować. Ta informacja to z europejskiego punktu widzenia bardzo złe wieści. Bowiem okazuje się, że ADVAPI uruchomi specjalne programy wstawione i kontrolowane przez NSA. Jak dotąd, nikt nie wie, czym są te

programy lub co tak naprawdę robią.

Dr Nicko van Someren informował, że na konferencji 98 Crypto, dokonał rozbioru na czynniki pierwsze sterownika ADVADPI. Znalazł w nim dwa różne klucze. Jeden był używany przez Microsoft do kontrolowania funkcji kryptograficznych włączonych w system Windows, w zgodzie z amerykańskimi przepisami eksportowymi. Ale przyczyna wbudowania drugiego klucza oraz tego, kto go posiada, pozostały tajemnicą.

DRUGI KLUCZ

Dwa tygodnie temu, amerykańska firma od bezpieczeństwa natknęła się na rozstrzygający dowód, że drugi klucz należy do NSA. Podobnie jak dr van Someren, Andrew Fernandez, główny naukowiec z Cryptonym w Morrisville, Północna Karolina, zajmował się wykrywaniem obecności i znaczeniem dwóch kluczy. Potem sprawdził najnowszą wersję dodatku Service Pack dla systemu Windows NT 4, pod nazwą Service Pack 5.

Odkrył, że programistom Microsoftu nie udało się usunąć lub "zatrzeć" symboli debugowania używanych do testowania tego oprogramowania, zanim znalazło się na rynku. Wewnątrz kodu były etykiety dla dwóch kluczy. Jeden nazywał się "KEY". Drugi był nazwany "NSAKEY".

Fernandes poinformował o swym ponownym odkryciu dwóch kluczy oraz ich tajnym znaczeniu na konferencji "Postępy w kryptologii, Crypto'99″ w Santa Barbara. Według obecnych na konferencji, programiści Windows uczestniczący w konferencji nie zaprzeczyli, że klucz "NSA" został wbudowany w ich oprogramowanie. Ale nie chcieli rozmawiać o tym, do czego ten klucz jest, i dlaczego został tam wprowadzony bez wiedzy użytkowników.

TRZECI KLUCZ?!

Jednak według dwóch świadków uczestniczących w konferencji, nawet najlepsi programiści Microsoftu od kryptografii ze

zdumieniem dowiedzieli się, że wersja ADVAPI.DLL znajdująca się w Windows 2000 zawiera nie dwa, ale trzy klucze.

Brian LaMachia, szef działu rozwoju kryptograficznego w Microsoft był "zdumiony", gdy dowiedział się o tych odkryciach od osób z zewnątrz. Najnowsze odkrycie dr van Someren jest oparte na zaawansowanych metodach wyszukiwania, które testują i informują o "entropii" kodu programowania.

W Microsofcie o dostępie do kodu źródłowego Windows mówi się, że jest bardzo „skategoryzowany", co ułatwia dokonywanie modyfikacji bez wiedzy nawet menedżerów poszczególnych produktów.

Naukowcy są podzieleni co do tego, czy klucz NSA może być przeznaczony do tego, aby rząd USA mógł wprowadzać do systemu Windows tajne kryptosystemy albo czy jest on przeznaczony do otwarcia wszystkich komputerów z systemem Windows na techniki zbierania danych wywiadu wykorzystywanych przez korpus "wojowników informacyjnych" NSA.

Według Fernandeza z Cryptonym, rezultatem istnienia tajnego klucza wewnątrz systemu operacyjnego Windows "jest to, żeby ogromnie ułatwić NSA załadowanie nieautoryzowanych usług do wszystkich kopii systemu Microsoft Windows, a gdy te usługi się tam znajdą, mogą one skutecznie opanować cały system operacyjny". Klucz NSA jest zawarty wewnątrz wszystkich wersji systemu Windows od Windows 95 OSR2 wzwyż.

"Dla nie-amerykańskich menedżerów IT polegających na Windows NT do obsługi wysoce poufnych centrów danych, to odkrycie jest bardzo niepokojące". "Rząd USA obecnie stara się utrudnić, jak się da, aby mocna kryptografia mogła być stosowana poza USA.

Zainstalowanie kryptograficznego back-door w najczęściej spotykanym systemie operacyjnym na świecie powinno dać silny impuls dla zagranicznych menedżerów IT". "Jak poczuje się taki człowiek, gdy dowiaduje się, że w każdej kopii systemu Windows, Microsoft ma "tylne drzwi" dla NSA – co ogromnie

ułatwia rządowi USA dostęp do komputera?” Czy taka luka się obróci się przeciw podglądaczom?

Autor: Duncan Campbell
Tłumaczenie: Pluszowy Miś
Źródło oryginalne: therebel.org
Źródło polskie: Stop Syjonizmowi