Nawet kabel twojego komputera może cię szpiegować!

31 grudnia 2013

Agencja NSA ma cały zestaw narzędzi przeznaczonych do łamania zabezpieczeń routerów, firewalli i innych produktów znanych firm. Agenci potrafią też podrzucić pluskwę na zamówiony komputer, zanim trafi on w przesyłce do odbiorcy – donosi niemiecki „Spiegel".

Osoby śledzące doniesienia o dokumentach od Edwarda Snowdena powinny już znać nazwę TAO albo Tailored Access Operations. Jest to specjalny wydział NSA zatrudniający setki hackerów i angażowany do szczególnie trudnych cybermisji. Poprzednie wycieki mówiły, że TAO mogła stać za zainfekowaniem tysięcy sieci, także w Polsce. Ten sam wydział prawdopodobnie szpiegował zagranicznych polityków.

Niemiecki „Spiegel" opublikował dość dużo materiałów na temat TAO, oczywiście bazujących na wyciekach Snowdena. Pierwszy długi artykuł dotyczy charakteru wydziału TAO oraz jego możliwości związanych m.in. ze szpiegowaniem użytkowników e-usług i dostępem do podmorskich kabli. Drugi, krótszy tekst dotyczy narzędzi stosowanych do łamania zabezpieczeń w stosowanych często produktach.

W doniesieniach „Spiegela" nie ma nic, co mogłoby bardzo nas zaskoczyć po wcześniejszych wyciekach. Możemy jednak poznać pewne szczegóły działań cyberszpiegów. Przykładowo Spiegel twierdzi, że agenci mogą zbierać informacje o każdej awarii systemu Windows na obserwowanym przez nich komputerze i mają dostęp do raportów o błędach, które użytkownik wysyła do Microsoftu.

Informacje z raportów o błędach są zbierane w systemie XKeyscore. Mają pozwalać na uzyskanie „pasywnego dostępu" do danej maszyny, czyli na śledzenie informacji wysyłanych z

komputera, ale bez manipulowania samą maszyną.

Nowe artykuły „Spiegela” wspominają też o narzędziach używanych do umieszczania szkodników na komputerach. Kiedyś NSA bazowała m.in. na lukach w IE, podobnie jak cyberprzestępcy. Z czasem zaszła potrzeba opracowania bardziej zaawansowanych narzędzi, a jeden ich zestaw nosi nazwę QUANTUMTHEORY. „Spiegel” twierdzi, że jedno z tych narzędzi – Quantuminsert – było używane w czasie opisywanych we wrześniu ataków na Belgacom.

Slajdy z prezentacji opisujące narzędzia QUANTUM wskazują jako potencjalny cel Facebooka, Yahoo, Twittera i YouTube. Najlepsze efekty osiągano przy próbach atakowania Facebooka i Yahoo. Najwyraźniej ta metoda nie sprawdziła się przy inwigilowaniu użytkowników usług Google.

Niemiecka gazeta pisze też, że uzyskała dostęp do 50-stronicowego katalogu, z którego agenci mogą zamówić rozwiązania do złamania zabezpieczeń w popularnych produktach. „Spiegel” twierdzi, że jeśli jakaś firma sięga po nowe zabezpieczenie (np. nowy firewall), wywiad już prawdopodobnie ma sposób na obejście go.

Katalog zawiera informacje o kosztach stosowania poszczególnych narzędzi. Te koszty wahają się od 0 do 250 tys. dolarów. Przykładowo spreparowany kabel, pozwalający widzieć, co jest wyświetlane na monitorze, kosztuje 30 dolarów. Aktywna stacja przekaźnikowa, pozwalająca na monitorowanie telefonów komórkowych na określonym terenie, to już koszt 40 tys. dolarów. Inne ciekawe rozwiązanie to wtyczka USB zdolna do wysyłania i odbierania informacji drogą radiową.

Za opracowaniem tych technologii ma stać specjalny wydział o nazwie ANT (od Access Network Technology). Jego narzędzia mają być stosowane tam, gdzie standardowe metody TAO zaczynają zawodzić.

ANT dostarcza nie tylko sprzęt, ale także oprogramowanie. Mogą

to być np. szkodniki atakujące BIOS komputera, których nie da się usunąć konwencjonalnymi metodami. ANT ma również dysponować narzędziami do atakowania routerów, firewalli, oprogramowania w urządzeniach znanych producentów itd. Spiegel wymienia produkty Cisco, Huawei, Della, Samsunga, Maxtora i in. Część z narzędzi szpiegowskich może być instalowana zdalnie, inne wymagają dostępu do urządzenia.
Tradycja i nowoczesność

Niemiecka gazeta twierdzi, że agenci NSA potrafią łączyć te cyfrowe zdobycze z tradycyjnymi metodami szpiegowania. Mogą przechwycić wysłany do kogoś komputer, ostrożnie otworzyć paczkę, zainstalować na urządzeniu pluskwę (w postaci oprogramowania lub sprzętu), by potem szpiegować swój cel w wygodny, zdalny sposób.

Trzeba mieć oczywiście na uwadze, że doniesienia Spiegela dotyczą działań przeciwko konkretnym osobom. NSA raczej nie instaluje pluskiew na przypadkowych komputerach. Poza tym część narzędzi opisana została tylko w slajdach i katalogach, a więc brakuje informacji o tym, jak często i w jaki sposób mogą być one wykorzystywane.

Autor: Marcin Maj
Źródło: Dziennik Internautów