MEC. ROBERT NOGACKI – jeden z najlepszych ekspertów w zakresie bezprawia urzędniczego – ocenia wydarzenia przez pryzmat interesów klientów swojej kancelarii.

Krótka droga od prowokacji do preparacji

Po niedawnej kompromitującej wpadce włoskiej firmy Hacking Team – producenta oprogramowania szpiegowskiego na potrzeby instytucji rządowych, który sam padł ofiarą hakerów – do internetu wyciekły tysiące poufnych dokumentów Hacking Team. Są wśród nich kody źródłowe, listy kontrahentów, jak również szczegóły korespondencji z klientami. Z tych informacji można się dowiedzieć, że klientem Hacking Team było m.in. polskie Centralne Biuro Antykorupcyjne, które nabyło licencję na opracowany przez Włochów program Remote Control System (RCS).

Hacking Team od lat zajmuje się produkcją specjalistycznego oprogramowania, służącego zdalnemu i skrytemu dostępowi do komputerów, urządzeń mobilnych oraz telefonów. W ujawnionych przez Wikileaks broszurach reklamowych Włosi chwalą się, że ich narzędzie pozwala nie tylko na monitorowanie czynności wykonywanych przez użytkowników na zainfekowanych komputerach, ale również na ingerowanie w te procesy w sposób niepozostawiający śladów.

Z tego zapewne powodu włoskim produktem zainteresowali się między innymi producent oprogramowania antywirusowego Kaspersky Lab oraz działające przy Uniwersytecie w Toronto Citizen-Lab, którego celem jest monitorowanie internetu pod kątem naruszania praw człowieka. Specjaliści z obu instytucji prześledzili nie tylko budowę szkodliwego oprogramowania, ale również sposób jego rozprzestrzeniania oraz źródła ataku.

Konkluzja jest prosta – zakupione przez CBA narzędzie to oprogramowanie do organizowania prowokacji i szpiegowania obywateli, a nie do zbierania materiału dowodowego w sprawach karnych. Różnica jest fundamentalna, ponieważ oprogramowanie służące do zbierania materiału dowodowego musi przede wszystkim gwarantować, że żadna osoba trzecia (w tym osoba prowadząca analizę) nie jest w stanie ingerować w treść danych w taki sposób, aby usunąć coś z materiału dowodowego albo coś do niego dodać. Takie procedury dają gwarancję, że materiał dowodowy jest autentyczny, a nie spreparowany przez służby specjalne. Natomiast RCS to program, który służy właśnie do ingerowania w dane umieszczone w komputerze, tak aby nie zostawiać po tej ingerencji śladów – ten program nie jest w stanie wytworzyć żadnych dowodów mających wartość sądową, a kluczem marketingu producenta programu jest deklaracja, że RCS pozwala ingerować w cudzy komputer, nie pozostawiając śladów.

Specjaliści z Kaspersky Lab podsumowali to w następujący sposób: „RCS nie ma żadnego mechanizmu, który pozwalałby na dokładne skopiowanie zawartości systemu plików lub skopiowanie zawartości pamięci RAM. Oznacza to, że wykonywanie losowego kodu w systemie (uaktualnienia i instalacje sterowników) nie określi jednoznacznie, czy jakiekolwiek nielegalne treści na komputerze zostały pobrane przez samego podejrzanego, czy przez operatora narzędzia RCS. Nie wydaje nam się, aby ten program mógł być używany do gromadzenia informacji, które mogłyby być wykorzystane jako dowód popełnienia bezprawnych działań. Zasadniczo program ma dość dziwną funkcję: robi to, czego nie powinien robić, a nie to, co powinien robić program, który zbiera dane do badań kryminalistycznych".

Wielu obywatelom naszego kraju CBA kojarzy się z wątpliwymi z moralnego i prawnego punktu widzenia prowokacjami. Teraz okazuje się, że ta sama instytucja posługuje się narzędziem operacyjnym, którego zastosowanie uniemożliwia określenie, czy modyfikacje zawartości twardego dysku lub pamięci komputera są dziełem jego użytkownika, czy też operatora narzędzia spyware, np. z CBA. Tym samym uzyskane w ten sposób dowody jako niegwarantujące autentyczności są pozbawione wartości procesowej. Dla porównania, EnCase Forensic, najpopularniejszy program służący do analizy dysków w celu pozyskania materiału dowodowego, tworzy sumę kontrolną dla wszystkich danych na analizowanym dysku, aby mieć gwarancję, że w toku analizy nikt nie zmienił przecinka.

Pytanie więc brzmi: w jakim celu CBA zakupiło program, którego posiadanie naraża tę instytucję na zarzut manipulowania dowodami? Dlaczego w sytuacji, gdy ma ono działać w ramach ściśle określonych reguł prawnych, wydaje znaczne sumy na zakup, którego zgodnie z tymi regułami nie może w pełni wykorzystać? Biorąc pod uwagę, że innymi użytkownikami RCS są rządy takich krajów jak Rosja, Sudan, Turkmenistan czy Egipt, odpowiedź może być na tyle szokująca, że lepiej nie wypowiadać jej głośno. ■

Mec. Robert Nogacki, założyciel Kancelarii Prawnej Skarbiec

BAROMETR PRZEDSIĘBIORCY

TAK

Polskie służby specjalne rozpoczęły zaciętą walkę z cyberprzestępcami. W ramach Agencji Bezpieczeństwa Wewnętrznego w 2014 r. powołano Rządowy Zespół Reagowania na Incydenty Komputerowe o nazwie CERT. Eksperci z CERT udaremnili w 2014 r. 119 akcji hakerów komputerowych na serwery administracji publicznej, czyli aż o 350 proc. więcej niż w 2013 r. Wśród nich były tzw. kampanie phishingowe, czyli zakrojone na szeroką skalę ataki polegające na tym, że przestępcy pod przykrywką znanych firm dokonywali włamań na serwery rządowe. Wystarczyło kliknąć na logo umieszczone w otrzymanym e-mailu, aby złośliwe oprogramowanie uzyskało dostęp do wszelkich danych znajdujących się na serwerze, w tym informacji podlegających szczególnej ochronie ze względu na interes państwowy.

NIE

Międzynarodowy Fundusz Walutowy w wydanym raporcie opiniującym stan polskiej gospodarki ocenił, że Polska nie powinna rezygnować z podwyższonych stawek podatku VAT. Przypomnijmy, że obecnie obowiązujące stawki 8 proc. i 23 proc. mają przestać obowiązywać w 2017 r. Dodatkowo MFW zalecił ujednolicenie stawek VAT w polskim systemie podatkowym, co zapewne ma się sprowadzać do nałożenia stawki 23 proc. na uprzywilejowane dotychczas towary i usługi. Naszym zdaniem eskalacja opodatkowania VAT w Polsce będzie przyczyną rozwoju... co najwyżej szarej strefy.

SKARBIEC KANCELARIA PRAWNA

MATERIAŁ: KANCELARIA PRAWNA SKARBIEC