**Kaspersky Lab otrzymuje patent na autorską technologię wykrywania zagrożeń w spakowanych plikach**

**Kaspersky Lab informuje, że uzyskał amerykański patent na system wykrywania szkodliwych programów zmodyfikowanych przy pomocy pakerów lub narzędzi służących do szyfrowania, które nie zostały jeszcze zidentyfikowane przez badaczy.**

Technologia ta została już zintegrowana z kluczowymi rozwiązaniami bezpieczeństwa firmy, przeznaczonymi dla użytkowników indywidualnych i korporacyjnych.

Pakery i narzędzia szyfrujące (które można uznać za rodzaj pakerów) tworzą plik kontenera, który zawiera wersję oryginalnego programu oraz kod niezbędny do rozpakowania lub odszyfrowania go.

Cyberprzestępcy wykorzystują takie narzędzia w celu modyfikowania szkodliwego oprogramowania, aby utrudnić jego wykrycie przez rozwiązania bezpieczeństwa. Technika ta pozwala im zmienić pliki binarne programu w celu obejścia skanerów antywirusowych opartych na sygnaturach. Nawet jeśli produkt bezpieczeństwa zawiera w swojej antywirusowej bazie danych sygnaturę dla oryginalnej próbki szkodliwego oprogramowania, nie będzie w stanie wykryć skompresowanej wersji takiego szkodliwego programu.

Programy zmodyfikowane przy użyciu popularnych pakerów mogą być wykrywane przy użyciu reguł heurystyki; jeśli jednak osoby atakujące stworzą swój własny paker przy użyciu unikatowego algorytmu, wykrycie zagrożenia stanie się znacznie trudniejsze. Technologia firmy Kaspersky Lab zawiera metodę analizowania obiektów, która tworzy specjalny profil dla każdego nowego pakera, zapewniając ogólny opis jego zachowania. Dzięki takiemu profilowi rozwiązanie bezpieczeństwa może następnie wykrywać szkodliwe oprogramowanie zmodyfikowane przy użyciu pakera na podstawie operacji, jakie wykonuje po uruchomieniu.

W praktyce mechanizm ten działa w następujący sposób: najpierw rozwiązanie antywirusowe stwierdza – przy użyciu własnego zestawu reguł – że analizowany podejrzany plik mógł zostać zmodyfikowany przy pomocy nieznanego dotąd pakera, a następnie odwołuje się do autorskiej, opatentowanej przez Kaspersky Lab metody. Technologia ta emuluje wykonanie skanowanego pliku i rejestruje wszystkie operacje wykonywane przez kod odpowiedzialny za odszyfrowanie i uruchomienie szkodliwego oprogramowania. Operacje te są klasyfikowane i poddawane analizie w celu stworzenia szablonów określających zachowanie pakera. Na ostatnim etapie wygenerowane dane służą do utworzenia profilu, który może być następnie wykorzystany do wykrywania innych plików zmodyfikowanych przy użyciu danego pakera.

*„O ile w przeszłości analizowanie zachowania pakerów było niepraktyczne i znacznie utrudnione, dzięki naszej technologii można analizować obiekty w sposób bardziej szczegółowy, co zwiększa jakość ochrony oferowanej użytkownikom. Ponadto, technologia ta zawiera metodę opisu zachowania nieznanych dotychczas pakerów w formie, która może być wykorzystywana przez rozwiązanie bezpieczeństwa, a jednocześnie jest czytelna dla analityków”* – powiedział Maksym Golowkin, ekspert ds. szkodliwego oprogramowania, Kaspersky Lab oraz autor nowo opatentowanej technologii.

Nowa technologia została już zaimplementowana w takich flagowych produktach firmy Kaspersky Lab jak [Kaspersky Internet Security](http://kaspersky.pl/kis) i [Kaspersky Endpoint Security for Business](http://kaspersky.pl/biznes).

Dział badań i rozwoju firmy Kaspersky Lab posiada personel liczący około tysiąca osób, co pozwala firmie rozwijać przełomowe technologie, z których wiele zostaje opatentowanych. Na początku października 2013 r. portfolio Kaspersky Lab zawierało 174 patentów wydanych w Stanach Zjednoczonych, Rosji, Unii Europejskiej i Chinach. Urzędy rozpatrują kolejne 211 wniosków patentowych.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.