**Kaspersky Lab patentuje zaawansowaną technologię pozwalającą na szybsze wykrywanie nieznanych zagrożeń**

**Kaspersky Lab informuje o opatentowaniu w Stanach Zjednoczonych autorskiej architektury bazy danych, która znacznie przyspiesza emulację systemu plików i rejestrów systemu.**

Patent opisuje hierarchiczną, zorientowaną obiektowo bazę danych, która została zaprojektowana do pracy z emulatorami. Ten rodzaj bazy danych umożliwia szybsze, proaktywne wykrywanie nieznanych jeszcze niebezpiecznych aplikacji.Jeśli bazy danych produktu antywirusowego nie zawierają sygnatury dla określonej aplikacji, nie musi to oznaczać, że program taki jest bezpieczny. Emulatory wbudowane w wiele rozwiązań antywirusowych mogą sprawdzić ‘doświadczalnie’, czy aplikacja na komputerze jest szkodliwa. Emulator tworzy środowisko wirtualne (wirtualną kopię systemu operacyjnego), uruchamia w nim potencjalnie szkodliwą aplikację i śledzi jej zachowanie. Jeśli zachowanie aplikacji zostanie uznane za szkodliwe, zostanie ona zablokowana, co zapobiegnie infekcji.

Emulacja systemu operacyjnego jest uznawana za efektywną metodę walki ze szkodliwym oprogramowaniem, a metody jej wdrażania różnią się. Działanie emulatora w dużej mierze zależy od rodzaju bazy danych używanej do utworzenia wirtualnej kopii systemu.

W procesie tworzenia wirtualnej kopii systemu emulator używa swego rodzaju ‘mapy’ składników systemu – bazy danych zawierającej informacje o tych składnikach i ich położeniu. Wydajność emulatora zależy bezpośrednio od tego, jak szybko jest on w stanie znaleźć dany składnik.

Wiele istniejących emulatorów używa relacyjnych baz danych, w których informacje są uporządkowane w tabelach. Wyszukiwanie w tych bazach może być powolnym procesem ze względu na metody wykorzystywane do obsługi danych zorganizowanych w taki sposób. Jednocześnie, podczas działania, próbki współczesnych szkodliwych programów mogą używać setek, a nawet tysięcy różnych plików systemu operacyjnego. W rezultacie, proces tworzenia środowiska wirtualnego do skanowania potencjalnie szkodliwego oprogramowania przy pomocy emulatora, wykorzystującego relacyjną bazę danych do przechowywania obiektów wirtualnego systemu plików, może zająć sporo czasu. Nie pozostanie to bez wpływu na wydajność rozwiązania antywirusowego i całego chronionego systemu operacyjnego.

**Przyspieszenie działania ochrony**

Architektura bazy danych, opatentowana przez ekspertów z Kaspersky Lab, posiada strukturę drzewiastą, która pozwala na bardziej wydajne rozmieszczenie danych. Emulator nie przeszukuje obszernych tabel w relacyjnej bazie danych, ale szybko odnajduje obiekt w strukturze hierarchicznej, określając ścieżkę dostępu do tego obiektu w oparciu o jego rodzaj oraz dodatkowe odniesienia między różnymi pozycjami w bazie danych.

Według wewnętrznych badań Kaspersky Lab, pełne przeszukanie bazy danych, zawierającej około 500 000 obiektów, zajmuje mniej niż sekundę. Warto tutaj nadmienić, że emulacja systemu operacyjnego Windows 7 w jego domyślnym stanie, bez żadnych dodatkowych aplikacji, wykorzystuje około 50 000 plików.

Korzyści płynące z opatentowanej technologii są oczywiste – dzięki nowej architekturze bazy danych produkty Kaspersky Lab mogą przeprowadzać analizę zachowania nieznanych programów w środowisku wirtualnym znacznie szybciej niż emulatory, które używają baz danych opartych na tradycyjnych metodach porządkowania danych.

Pomimo tego, że patent został opublikowany dopiero pod koniec marca 2013 r., technologia ta działa już w następujących produktach Kaspersky Lab: Kaspersky Internet Security 2013, Kaspersky PURE 3.0, Kaspersky Endpoint Security for Windows, Kaspersky Security for Virtualization, Kaspersky Anti-Virus for Mac, Kaspersky Endpoint Security for Mac, Kaspersky Anti-Virus for Lotus Notes, Kaspersky Anti-Virus for Microsoft ISA Server/Forefront TMG oraz Kaspersky Security for Linux Mail Server.

Firma Kaspersky Lab stale powiększa swoją własność intelektualną. Na początku marca 2013 r. portfolio firmy zawierało ponad 130 patentów opublikowanych w Stanach Zjednoczonych, Rosji, Unii Europejskiej i Chinach. Dodatkowo, 200 zgłoszeń patentowych jest aktualnie rozważanych przez urzędy patentowe w tych krajach.

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