NOWA RECEPTA NA CYBERATAKI WYMIERZONE W FIRMY

Kaspersky Lab udostępniło nowe narzędzie Anti Target Attack Platform. Jest to rozwiązanie, które ma wykrywać ataki ukierunkowane.

Konwencjonalne technologie ochrony dobrze radzą sobie z zapobieganiem typowym zagrożeniom oraz atakom. Chociaż zagrożenia te stanowią mniej niż 1 proc, to wystawiają firmy na całym świecie na ryzyko. Co więcej, liczba takich ataków stale rośnie przy jednoczesnym spadku cen narzędzi do przeprowadzeniu skutecznej akcji.

Anti Targeted Attack Platform ma na celu zidentyfikować i zwrócić uwagę na nietypowe działania, które stanowią mocny dowód na "złośliwe" intencje, w oparciu o analizę korporacyjnej aktywności sieciowej oraz z wykorzystaniem źródeł danych o aktywności cyberprzestępców. Czujniki rozwiązania odpowiadają za zbieranie danych w ruchu sieciowym, WWW oraz e-mail, jak również na punktach końcowych.

Podejrzane zdarzenia są następnie przetwarzane przy użyciu różnych mechanizmów, łącznie z zaawansowaną piaskownicą (sandbox) i narzędziem analizy ataków ukierunkowanych, w celu uzyskania ostatecznego werdyktu.

Narzędzie analizy ataków ukierunkowanych wykorzystuje technologie przetwarzania danych oraz uczenia się w celu oceny i łączenia werdyktów z różnych mechanizmów analizy. Dodatkowe technologie, które pomagają ograniczyć fałszywe alarmy, obejmują silnik antywirusowy firmy pozwalający wykluczyć typowe ataki, system wykrywania włamań oraz obsługę niestandardowych reguł umożliwiających wykrywanie określonej aktywności w sieci korporacyjnej.

– Opracowując Anti Targeted Attack Platform, mieliśmy świadomość, że w skutecznym rozwiązaniu nie może zabraknąć znanych i skutecznych mechanizmów bezpieczeństwa. Jednocześnie nowe zagrożenia korporacyjne wymagają zaawansowanej technologii i analizy na znacznie wyższym poziomie niż w przypadku konwencjonalnych rozwiązań. Efektem naszych starań, wiedzy i talentu jest produkt, który pomaga przedsiębiorstwom osiągnąć nowy poziom bezpieczeństwa infrastruktury IT – mówi Nikita Szewcow z Kaspersky Lab.

Źródło: Kaspersky Lab

Czytaj też: Kampania phishingowa wymierzona w PGE nadal trwa