**Nowe rozwiązanie firmy Check Point zapewnia bezprecedensowy stopień bezpieczeństwa systemów informatycznych**

**SandBlast™ firmy Check Point podnosi poprzeczkę w grze o bezpieczeństwo systemów informatycznych, oferując metodę wykrywania zagrożeń w odpornym na mechanizmy maskujące środowisku testowym oraz system filtrowania dokumentów Threat Extraction**

Dzięki zastosowaniu metody wykrywania zagrożeń na poziomie procesora jeszcze zanim dojdzie do zainfekowania systemu, SandBlast firmy Check Point oferuje wyższy poziom bezpieczeństwa. System wykrywania szkodliwego oprogramowania odporny na mechanizmy maskujące oraz kompleksowe zabezpieczenia nawet przed najgroźniejszymi atakami znacząco zmniejszają ryzyko kosztownych włamań do systemów informatycznych.

W nieustającej wojnie między hakerami i specjalistami od bezpieczeństwa systemów komputerowych napastnicy stosują coraz bardziej zaawansowane narzędzia, takie jak nowe metody ataku wykorzystujące luki „zero-day” oraz zmodyfikowane wersje znanego już złośliwego oprogramowania, zdolne przeniknąć do atakowanej infrastruktury, mimo istnienia tradycyjnych systemów wykrywania zagrożeń w środowisku testowym („piaskownicy”).

Te nowe metody ataku wymagają aktywnej obrony przy użyciu nowoczesnych rozwiązań i technologii, zdolnych do wykrywania nie tylko znanych zagrożeń, ale także nowego, nieznanego dotąd szkodliwego oprogramowania. W nowym rozwiązaniu firmy Check Point wykorzystano ultranowoczesną technologię wykrywania exploitów na poziomie procesora (CPU), dzięki czemu jest ono jedynym produktem na rynku wykrywającym najbardziej niebezpieczne zagrożenia „zero-day”, jeszcze zanim szkodliwe oprogramowanie zainfekuje system i uruchomi mechanizmy maskujące jego obecność.

— Trwa cybernetyczna wojna i jedynym sposobem obrony przed nowymi zagrożeniami jest stworzenie systemu aktywnych zabezpieczeń, pozwalającego osiągnąć maksymalny poziom bezpieczeństwa bez zmniejszania efektywności operacyjnej — stwierdził Mike Stiglianese, dyrektor zarządzający Axis Technology LLC i były dyrektor ds. technologii w dużej instytucji finansowej. — Oferując nowe metody wykrywania zagrożeń na poziomie procesora, Check Point podnosi poprzeczkę, tworząc nowatorskie i kompleksowe rozwiązania w zakresie bezpieczeństwa systemów informatycznych, stanowiące najbardziej zaawansowaną broń

w walce z nowymi, wyspecjalizowanymi metodami ataku.

— *W szybko zmieniającym się krajobrazie zagrożeń konieczne jest stosowanie skutecznych środków bezpieczeństwa. Nowa technologia, która chroni infrastrukturę niezbędną do funkcjonowania naszej firmy przed nowszymi typami szkodliwego oprogramowania, a także zapewnia niezakłócony przepływ informacji, to wielki krok naprzód* — mówi Richard Peirce, dyrektor działu Infrastructure Services w firmie Boston Properties. — Zawsze starannie analizujemy warunki, jakie muszą zostać spełnione, aby wdrożyć nowy produkt w naszym środowisku. Oparte na technologii firmy Check Point rozwiązanie do wykrywania zagrożeń

w środowisku testowym („piaskownicy”) zostało sprawnie wdrożone, a podczas eksploatacji wymaga nadzoru administracyjnego tylko w ograniczonym zakresie.

Najważniejsze zalety rozwiązania SandBlast firmy Check Point:

l Wykrywanie szkodliwego oprogramowania na etapie exploitu, zanim jeszcze mogą zostać uruchomione mechanizmy maskowania jego obecności. System jest odporny na pętle opóźniające, próby wykrycia wirtualizacji systemu operacyjnego czy inne metody mające na celu uniknięcie wykrycia ataku w środowisku testowym.

l Łączy zaawansowane metody wykrywania zagrożeń na poziomie procesora z emulacją na poziomie systemu operacyjnego, umożliwiającą filtrowanie zawartości plików różnych typów, m.in. MS Office, PDF, flash, plików wykonywalnych i archiwów.

l Szybkie udostępnianie danych oczyszczonych z potencjalnie niebezpiecznej zawartości dzięki systemowi Threat Extraction, zapobiegającemu przeniknięciu szkodliwego oprogramowania do infrastruktury, bez powodowania znaczących opóźnień w obiegu dokumentów.

Rozwiązanie SandBlast firmy Check Point stanowi element nowej generacji produktów [Threat Prevention](http://www.checkpoint.com/products-solutions/threat-prevention/advanced-threat-prevention/index.html); w jego skład wchodzą produkty Threat Emulation i Threat Extraction. Threat Emulation integruje nową technologię wykrywania zagrożeń na poziomie procesora z systemem wykrywania szkodliwego oprogramowania w środowisku testowym („piaskownicy”) na poziomie systemu operacyjnego, którego skuteczność została niedawno potwierdzona. [Opierając się na wynikach przeprowadzonych testów, NSS Breach Detection Systems](http://www.checkpoint.com/press/2015/check-point-delivers-superb-advanced-threat-protection-in-latest-nss-labs-test/) zalicza produkt Threat Emulation firmy Check Point do grupy najbardziej wartościowych, „polecanych” rozwiązań, charakteryzujących się najwyższym poziomem skuteczności i wydajności. W skład nowego produktu wchodzi system Threat Extraction, zapewniający użytkownikom szybki dostęp do bezpiecznych wersji dokumentów, podczas gdy pierwotne pliki poddawane są testom. Integrując metody wykrywania zagrożeń na poziomie procesora z systemem Threat Extraction, produkt SandBlast firmy Check Point jeszcze bardziej podnosi poprzeczkę, przewyższając pod względem poziomu bezpieczeństwa wszystkie inne produkty dostępne na rynku.

— *Firmy są przedmiotem ukierunkowanych ataków, lecz wdrożenie aktywnych, prewencyjnych zabezpieczeń może zapobiec przeniknięciu szkodliwego oprogramowania do sieci i chronić zasoby firmy bez pogorszenia wydajności pracy. SandBlast firmy Check Point zapewnia dodatkowy poziom zabezpieczeń przed nawet najbardziej zaawansowanymi atakami, blokując szkodliwe oprogramowanie przy minimalnym opóźnieniu obiegu informacji* — twierdzi Gil Shwed, założyciel i prezes Check Point Software Technologies. — *Stale powiększający się portfel rozwiązań Threat Prevention pozwala naszym klientom skutecznie walczyć z przestępczością cybernetyczną za pomocą nowatorskich strategii obronnych, wykorzystujących coraz doskonalszą technologię. Check Point* [Mobile Threat Prevention](http://www.checkpoint.com/products/mobile-threat-prevention/index.html) *i Check Point podejmują szybkie i zdecydowane działania, aby zapewnić bezpieczną przyszłość.*