**Zabójcza broń na exploity: rozwiązanie korporacyjne Kaspersky Lab wyprzedza konkurencję**

**Rozwiązanie bezpieczeństwa firmy Kaspersky Lab przeznaczone dla użytkowników korporacyjnych - Kaspersky Endpoint Security for Business – udowodniło swoją skuteczność w teście Real World Enterprise Security Exploit Prevention Test.**

Test przeprowadzony został przez organizację MRG Effitas w okresie od listopada 2013 do lutego 2014 roku.

Exploity to szkodliwe programy, które wykorzystują luki w zabezpieczeniach (krytyczne błędy w kodzie) legalnego oprogramowania w celu przeniknięcia do komputera. Exploit zwykle atakuje system, gdy użytkownik dziurawych aplikacji odwiedza zainfekowaną stronę. Warto pamiętać, że każda strona może być zainfekowana, nawet taka, która jest znana i była już wcześniej odwiedzana. Exploit jest aktywowany bez wiedzy użytkownika, a jego uruchomienie nie wymaga pobrania pliku wykonywalnego na dysk komputera.

Dla użytkowników korporacyjnych exploity stanowią jeszcze większe zagrożenie, ponieważ atak na komputery firmy może zakłócić jej procesy biznesowe i spowodować ogromne straty – zarówno finansowe, jak i na reputacji. Wykorzystanie exploitów znacznie zwiększa efektywność cyberataków przeprowadzanych na konkretne organizacje. Jednym z nowszych przykładów exploitów jest szkodnik o nazwie Careto (znany również jako The Mask), który zaatakował co najmniej 380 publicznych i prywatnych celów o wysokim znaczeniu strategicznym na całym świecie. Ochrona klientów korporacyjnych jest wymagająca tym bardziej, że niektóre firmy muszą wykorzystywać oprogramowanie, które jest kompatybilne tylko ze starszymi - a tym samym bardziej podatnymi na ataki - wersjami Javy, dla której powstaje dzisiaj większość exploitów.

Eksperci z MRG Effitas zbadali poziom ochrony przed exploitami zapewnianej przez sześć produktów korporacyjnych pochodzących od różnych producentów. W przeciwieństwie do konkurencji, Kaspersky Endpoint Security for Business był testowany nie tylko jako produkt zintegrowany. Dodatkowo ocenie poddano jego moduł Automatyczne zapobieganie exploitom, który został przetestowany niezależnie od innych mechanizmów ochrony. Ta technologia ochrony przed exploitami jest obecnie wykorzystywana we wszystkich rozwiązaniach bezpieczeństwa firmy Kaspersky Lab.

Eksperci z MRG Effitas wybrali 110 szkodliwych odsyłaczy prowadzących do exploitów w celu przetestowania ochrony oferowanej przez różne produkty. Celem ogromnej większości (98) tych exploitów była platforma Java. Wzrost liczby takich exploitów w ciągu ostatnich dwóch lat był przedmiotem badania firmy Kaspersky Lab pod nazwą „[Java pod ostrzałem – ewolucja exploitów w latach 2012 – 2013](http://securelist.pl/threats/7250,java_pod_ostrzalem_ewolucja_exploitow_w_okresie_2012_2013.html)”.

Testy zostały przeprowadzone w dwóch etapach. W pierwszym określono odsetek exploitów zablokowanych we wczesnej fazie, zanim szkodliwy kod rozpoczął swoją niebezpieczną aktywność. Drugi etap był mniej rygorystyczny i oprogramowanie bezpieczeństwa „zaliczyło” test, nawet jeśli nie zablokowało pierwotnego exploita, ale zdołało odeprzeć dowolne szkodliwe oprogramowanie, które próbował załadować.

Kaspersky Endpoint Security for Business uzyskał najlepsze wyniki na pierwszym etapie, blokując 98% exploitów. Warto wspomnieć, że technologia Automatyczne zapobieganie exploitom, nawet gdy była testowana oddzielnie, bez udziału innych funkcji bezpieczeństwa, poradziła sobie lepiej niż większość innych uczestników testu i zajęła drugie miejsce ex aequo, po tym jak zablokowała 95% exploitów.

Na drugim etapie Kaspersky Endpoint Security for Business zablokowało 100% zagrożeń. Tylko jeden produkt konkurencyjny zdołał dorównać temu wynikowi – inne testowane rozwiązania powstrzymały nie więcej niż 94% zagrożeń. Wyniki testu Real World Enterprise Security Exploit Prevention pozwoliły rozwiązaniu korporacyjnemu firmy Kaspersky Lab uzyskać wyróżnienie MRG Effitas Certified.

**Oleg Iszanow**, dyrektor ds. badań dotyczących ochrony przed szkodliwym oprogramowaniem, Kaspersky Lab, powiedział: „Dzisiaj żaden poważny cyberatak na cele firmowe nie może zostać przeprowadzony bez udziału exploitów. Działając w sposób ukradkowy, exploity przejmują kontrolę nad komputerem i uruchamiają szkodliwy kod, który przeprowadza główną część ataku. Dlatego bezpieczniej jest zablokować exploita na pierwszym etapie, zanim załaduje na komputer szkodliwe programy. Test przeprowadzony przez MRG Effitas pokazał, że nasza technologia Automatyczne zapobieganie exploitom może poradzić sobie z tym zadaniem lepiej niż rozwiązania konkurencji, nawet bez pomocy innych zawartych w produkcie podsystemów bezpieczeństwa”.

Testy zostały przeprowadzone na 64-bitowej wersji systemu Microsoft Windows 7 Enterprise SP1. Na komputerach wykorzystanych do testów zostały zainstalowane również aplikacje, które były najczęściej atakowane przez exploity w zeszłym roku, takie jak Java 1.7, Adobe Reader 9.3, Flash Player 10.1, Silverlight 5.1 oraz Internet Explorer 8.0.

Pełny raport z testu jest dostępny na stronie <https://www.mrg-effitas.com/wp-content/uploads/2014/03/MRG-Effitas-Real-World-Enterprise-Security-Exploit-Prevention-Test-February-2014.pdf>.

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>.