Ochrona przed najnowszymi zagrożeniami dzięki funkcji Kontrola systemu firmy Kaspersky Lab

Dzisiejsze systemy komputerowe lepiej niż kiedykolwiek radzą sobie w pracy wielozadaniowej. Pozwalają na jednoczesną pracę wielu programów, z których każdy działa w określonym celu oraz posiada szereg przywilejów w systemie.

Zadaniem rozwiązania bezpieczeństwa jest blokowanie wszystkich destrukcyjnych aktywności programów, takich jak infekowanie innych plików lub dokonywanie niepożądanych zmian w systemie. Klasyczna metoda identyfikowania tego typu programów opiera się na wykrywaniu unikatowej sygnatury kodu, która definiuje wcześniej zidentyfikowane szkodliwe programy. Proces ten znany jest jako wykrywanie oparte na sygnaturach zagrożeń. Jednak korzystanie jedynie z metod opartych na sygnaturach nie zapewnia już skutecznej ochrony przed szkodliwymi programami. Według wewnętrznych danych firmy Kaspersky Lab, każdego dnia pojawia się około 325 000 nowych próbek szkodliwego oprogramowania, przy czym dla wielu z nich nie ma jeszcze sygnatur.

Istnieje skuteczna metoda zwalczająca tego typu zagrożenia. Polega ona na analizie zachowania aplikacji w systemie oraz wykrywaniu aktywności typowych dla szkodliwego oprogramowania. Jednak dane dotyczące każdego programu z osobna są fragmentaryczne i nie dają pełnego obrazu wszystkich zdarzeń mających miejsce w systemie.

Monitorowanie zdarzeń w systemie receptą na sukces

Technologia monitorowania zdarzeń w systemie stanowi nowy etap w rozwoju oprogramowania bezpieczeństwa, ponieważ oferuje wiarygodną i kompletną informację na temat systemu jako całości, co w rezultacie umożliwia maksymalną kontrolę nad szkodliwą aktywnością oraz, w razie konieczności, przywrócenie do normy operacyjnych parametrów systemu.

Funkcja monitorowania zdarzeń w systemie śledzi wszystkie ważne aktywności mające miejsce w systemie: zmiany wprowadzane w plikach systemu operacyjnego, zmiany konfiguracji, uruchamianie programów, wymiana danych w sieci itp. Wszystkie te zdarzenia są rejestrowane oraz poddawane analizie. Jeżeli w działaniu jakiegoś programu zostanie wykryte zachowanie charakterystyczne dla szkodliwych aplikacji, wszystkie czynności wykonywane przez ten program zostaną zablokowane, a dokonane zmiany cofnięte, co zapobiegnie dalszej infekcji.

Monitorowanie zdarzeń działa wszechstronnie i jest skuteczne w walce z wszelkiego rodzaju oprogramowaniem, które wykazuje oznaki destrukcyjnej aktywności w systemie. Oznacza to, że technologia ta może być wykorzystywana do wiarygodnego wykrywania nowych złośliwych programów, których sygnatury nie są jeszcze dostępne.

Kontrola systemu firmy Kaspersky Lab: jeszcze wyższy poziom ochrony

Produkty firmy Kaspersky Lab zawsze były oparte na zaawansowanych, przełomowych technologiach zwalczających zagrożenia. Podstawowa funkcja monitorowania systemu dostępna była już w 2009 r. w produktach dla klientów biznesowych. W kolejnych latach funkcja ta ewoluowała, przeobrażając się w technologię Kontrola systemu.

Funkcja Kontrola systemu skanuje dane związane z wykonywaniem najważniejszych czynności w systemie, monitorując procesy tworzenia i modyfikacji plików, działanie usług systemowych, wprowadzanie zmian do rejestru systemu, połączenia systemowe oraz transfer danych w sieci. Kontrola systemu monitoruje również informacje na temat symbolicznych operacji dotyczących plików lub katalogów, oraz chroni przed modyfikacjami rekordu rozruchowego przechowującego dane na temat procesu uruchamiania systemu operacyjnego oraz zabezpiecza przed przechwyceniem procesu restartu systemu. Ponadto, Kontrola systemu analizuje zawartość pakietów transmitowanych za pośrednictwem protokołu TCP (głównego protokołu służącego do przesyłania danych) w poszukiwaniu jakichkolwiek oznak przestępczej aktywności. Proces gromadzenia wszystkich danych jest automatyczny i nie wymaga interakcji użytkownika.

Korzystając z modułu BBS (Behaviour Stream Signatures), Kontrola systemu, na podstawie przeanalizowanych danych, może samodzielnie decydować o tym, czy dany program jest szkodliwy. Dodatkowo, produkty firmy Kaspersky Lab zawierają mechanizm, poprzez który moduł BSS nieustannie wymienia informacje z innymi komponentami tj. Ochrona WWW, Ochrona komunikatorów, technologia Host Intrusion Prevention System oraz zapora sieciowa. W rezultacie, rozwiązanie bezpieczeństwa gwarantuje lepszy poziom wykrywania szkodliwego oprogramowania oraz incydentów naruszenia polityki prywatności, gdyż skuteczniej potrafi identyfikować sekwencje zdarzeń prowadzące do tego typu problemów.

Kontrola systemu podlega całkowitej aktualizacji. Mechanizmy zapisujące listy zdarzeń oraz ich monitoring, a także mechanizmy heurystyczne, mogą być modyfikowane i dostosowane do potrzeb. Gwarantuje to szybkość procesu adaptacji do nieustannie zmieniających się zagrożeń oraz konfiguracji systemów komputerowych. Uaktualnienia Kontroli systemu są pobierane wraz z regularnymi aktualizacjami baz danych sygnatur zagrożeń i nie wymagają poświęcania dodatkowego czasu, ani żadnego zaangażowania ze strony użytkownika.

Wykrywanie zagrożeń

Wbudowany moduł BSS decyduje o szkodliwości danego programu poprzez porównanie jego prawdziwego zachowania z modelami szkodliwego zachowania. Analiza oraz ewentualna klasyfikacja programu jako szkodliwego odbywa się w czasie rzeczywistym. Rozwiązania Kaspersky Lab posiadają także funkcję wykrywania heurystycznego w oparciu o moduł BSS, dzięki czemu mogą wychwycić zachowanie podobne do szkodliwego, lecz w rzeczywistości niekoniecznie nim będące. Poza standardowymi metodami wykrywania, Kontrola systemu identyfikuje także potencjalnie szkodliwe akcje. Przykładowo, jeżeli

zaufana aplikacja uruchamia szkodliwy kod w wyniku ataku exploita, produkt bezpieczeństwa wykryje to zdarzenie oraz doradzi użytkownikowi zablokowanie podejrzanej czynności.

Użytkownik może wybrać pomiędzy trybem całkowicie automatycznym lub interaktywnym. W trybie interaktywnym użytkownik posiada szerszy wybór opcji działania.

Podsystem przeciwdziałania oprogramowaniu typu cryptomalware

Wzrastająca liczba oprogramowania typu cryptomalware, które szyfruje dane użytkownika i żąda pieniędzy w zamian ich odszyfrowanie, doprowadziła do zaistnienia niezwykle pilnej potrzeby opracowania metody zwalczania tego typu ataków. W odpowiedzi na to firma Kaspersky Lab zaimplementowała odpowiednią technologię w module Kontrola systemu. Dzięki niej możliwe jest cofnięcie konsekwencji ataku oprogramowania typu cryptomalware. W momencie wykrycia podejrzanej aplikacji usiłującej otworzyć poufne pliki użytkownika produkt firmy Kaspersky Lab natychmiast tworzy kopię zapasową tych plików. Nie ma więc potrzeby odszyfrowywania żadnych danych, gdyż istnieje ich kopia zapasowa, którą można je zastąpić.

Ochrona przed aplikacjami blokującymi ekran

Aplikacje blokujące ekran to kolejny rodzaj oprogramowania wyłudzającego pieniądze. Ich działanie polega na zablokowaniu dostępu do funkcji komputera poprzez pojawienie się na ekranie banera z żądaniem okupu, którego nie da się zamknąć ani przenieść. W ustawieniach Kontroli systemu istnieje odpowiednia opcja włączająca funkcję ochrony przed tego typu oprogramowaniem poprzez ustalenie kombinacji klawiszy, które należy wcisnąć w celu zamknięcia banera. Wciśnięcie ustalonych klawiszy nie tylko zamyka niechciany baner, lecz także całkowicie usuwa szkodliwe oprogramowanie odpowiedzialne za jego pojawienie się. Domyślnie funkcja ta jest aktywna.

Podsystem automatycznej ochrony przed exploitami

Następnym elementem wchodzącym w skład Kontroli systemu jest moduł Automatycznej ochrony przed exploitami, który przeciwdziała oprogramowaniu wykorzystującemu luki w zabezpieczeniach programów oraz dokonującemu tak zwanych ataków zero-day. Moduł ten kontroluje różne aplikacje, zwracając szczególną uwagę na te będące najczęstszym celem ataków, oraz dodatkowo sprawdza, czy nie usiłują one uruchomić żadnego podejrzanego kodu. Zebrane w ten sposób informacje pomagają wykryć, a następnie zablokować działania charakterystyczne dla exploitów. Dodatkowo, Automatyczna ochrona przed exploitami korzysta z technologii Forced Address Space Layout Randomization, która utrudnia exploitom zlokalizowanie w pamięci ich własnego szkodliwego kodu, dzięki czemu zapobiega

wykorzystaniu luk. Szczegółowe informacje na temat tej technologii są dostępne na stronie: http://kaspersky.pl/images/news/klp_whitepaper_aep.pdf.

Moduł kontroli aplikacji Javy

Ochrona przed lukami występującymi w platformie Java od zawsze stanowiła jedną z istotniejszych kwestii bezpieczeństwa z racji popularności tego środowiska. Aby wykryć atak usiłujący wykorzystać lukę w Javie, Kontrola systemu posiada specjalny moduł Java2SW, który ma bezpośredni dostęp do platformy oraz wprowadza dodatkowy element ochrony w każdej maszynie wirtualnej Javy. Java2SW dokładnie analizuje kod oraz zatrzymuje jego uruchomienie w momencie wykrycia jakiejkolwiek podejrzanej aktywności.

Cofanie niechcianych zmian w systemie

Zaraz po wykryciu infekcji Kontrola systemu inicjuje cofnięcie zmian wprowadzonych przez szkodliwe oprogramowanie (np. powrót do poprzednich, bezpiecznych parametrów systemu). Cofanie zmian w systemie obejmuje tworzenie i modyfikację plików wykonywalnych, modyfikacje dokonane w MBR, plikach Windows oraz kluczach rejestru. W najnowszych wersjach produktów firmy Kaspersky Lab istnieje możliwość aktualizacji mechanizmów cofających niechciane zmiany w systemie.

Dostępność

Technologia Kontrola systemu jest dostępna w produktach dla klientów indywidualnych i biznesowych:

Ochrona dla domu:

- Kaspersky Internet Security
- Kaspersky Internet Security – multi-Device (tylko dla systemu Windows)
- Kaspersky Total Security – multi-Device (tylko dla systemu Windows)
- Kaspersky Anti-Virus

Ochrona dla biznesu:

- Kaspersky Endpoint Security for Business
- Kaspersky Small Office Security

Podsumowanie

Monitorowanie systemu komputera oraz jego implementacja za pomocą modułu Kontrola systemu obrazuje podejście firmy Kaspersky Lab do kwestii bezpieczeństwa. Wszystkie ważne czynności wykonywane w systemie są monitorowane, dzięki czemu możliwe jest wykrycie szkodliwego oprogramowania.

Dzięki tej metodzie ochrony, możliwe jest zablokowanie wszelkich szkodliwych działań programów, bez względu na to, czy istnieje już sygnatura zagrożeń przypisana do ich kodu. Posiada ona także wysoki współczynnik wykrywania przy znikomej ilości fałszywych trafień, gdyż destrukcyjne działanie jest najbardziej wiarygodną cechą charakteryzującą szkodliwy program.

Ciągłe i szczegółowe monitorowanie systemu komputera pozwala na dokładne cofnięcie szkód wyrządzonych przez szkodliwe oprogramowanie. Przyczynia się to także do jeszcze wiarygodniejszej oceny ogólnego poziomu bezpieczeństwa komputera, co pozwala na skuteczniejsze diagnozowanie stanów i procesów nietypowych z punktu widzenia bezpieczeństwa.