KASPERSKY lab

Technologia Automatyczne zapobieganie exploitom

Podejście Kaspersky Lab do bezpieczeństwa opiera się na ochronie wielowarstwowej. Większość szkodliwych programów powstrzymuje pierwsza warstwa – zostają np. zidentyfikowane za pomocą wykrywania opartego na sygnaturach. Istnieją jednak szkodliwe obiekty, które wymagają specjalnego „traktowania”: w przypadku, gdy zdołają obejść jedną warstwę ochrony, trzeba zadbać o to, aby zostały wykryte przez następną. Na przykład, jeśli złożone szkodliwe oprogramowanie jest całkowicie nowe i jego sygnatura nie jest jeszcze znana, może zostać zablokowane przez system Kaspersky Security Network, który uzyskuje informacje dotyczące nowych cyberataków od milionów użytkowników, którzy dobrowolnie zgodzili się wysyłać do chmury Kaspersky Lab informacje o szkodliwej aktywności na ich komputerach. Kolejną warstwę stanowi szeroki wachlarz technologii ochrony proaktywnej, który analizuje kod podejrzanych aplikacji. Nawet jeśli aplikacja zdołała uruchomić się w chronionym systemie, rozwiązanie bezpieczeństwa będzie śledzić jej działania i zablokuje wszelką niebezpieczną aktywność przy pomocy modułu Kontrola systemu.

Kolejny obszar cyberprzestępczości, który według nas wymaga nowej specjalnej warstwy ochrony, stanowią exploity, wykorzystujące luki w popularnym oprogramowaniu. Cyberprzestępcy wykorzystują zarówno dobrze znane, jak i nowe luki w oprogramowaniu (tzw. luki „zero-day”, dla których nie istnieją jeszcze łaty) takim jak Adobe Flash, Adobe Reader, Java Runtime Environment, przeglądarki internetowe oraz w głównych komponentach systemu Windows jako bramę, poprzez którą można uruchomić na komputerach ofiar szkodliwy kod. Exploity wykorzystujące luki w zabezpieczeniach są powszechnie stosowane w szkodliwym oprogramowaniu, ale również stanowią podstawę dla ataków ukierunkowanych, które są trudne do wykrycia i zablokowania przy użyciu konwencjonalnych metod ochrony. Nasza wyspecjalizowana warstwa ochrony opiera się na technologii *Automatyczne zapobieganie exploitom* i stanowi całkowicie nowy, niezwykle skuteczny sposób wykrywania nowych oraz nieznanych exploitów.

Typowe zachowanie exploitów

Celem każdego exploita jest wykorzystanie określonych luk w zabezpieczeniach oprogramowania w celu wykonania różnego rodzaju szkodliwego kodu. Aby system mógł zostać zainfekowany za pośrednictwem „dziurawego” oprogramowania, użytkownik musi zostać zwabiony na szkodliwą stronę internetową (lub legalną stronę, która została tak spreparowana, aby zawierała szkodliwy moduł) lub pobrać i otworzyć specjalnie przygotowany dokument (dokument Microsoft Office, plik PDF, a nawet obrazek, który wydaje się nieszkodliwy). Szkodliwe odsyłacze prowadzące do zainfekowanych stron internetowych lub plików mogą być rozprzestrzeniane za pośrednictwem poczty e-mail, komunikatorów internetowych lub portali społecznościowych i można je nawet znaleźć w wynikach wyszukiwania dla popularnych zapytań. Typowe ataki ukierunkowane zwykle zostają uruchomione w momencie otwarcia przez użytkownika specjalnie utworzonego załącznika e-mail, który na pierwszy rzut oka często wygląda na całkowicie legalny.

Najczęściej atakowane oprogramowanie

Niemal każda aplikacja jest podatna na występowanie błędów w oprogramowaniu, a niektóre z nich mogą prowadzić do nieautoryzowanego wykonania szkodliwego kodu. Jednak

cyberprzestępcy zwykle biorą na celownik jedynie te programy, które są zainstalowane na niemal każdym komputerze – co gwarantuje im ogromną liczbę potencjalnych ofiar.

Ogólne środki ochrony przed exploitami

Rozwiązania bezpieczeństwa, takie jak Kaspersky Internet Security, wykorzystują różne metody w celu blokowania exploitów. Dodawane są specjalne sygnatury dla exploitów, które pomagają wykrywać szkodliwe pliki (na przykład w załączniku do poczty e-mail) jeszcze przed ich otwarciem. Ochrona proaktywna oraz inne technologie umożliwiają wykrywanie i blokowanie szkodliwej funkcji, nawet jeśli niebezpieczny plik został już uruchomiony. Ponadto, funkcja skanowania luk w zabezpieczeniach pozwala użytkownikom zidentyfikować dziurawe oprogramowanie i doradza, w jaki sposób należy je uaktualnić. Naturalnie, wykonywanie regularnych aktualizacji komponentów systemu Windows oraz zainstalowanego oprogramowania jest najlepszym sposobem na uniknięcie większości exploitów.

W niektórych przypadkach ogólne techniki ochrony mogą nie być skuteczne. Dotyczy to w szczególności luk zero-day – czyli takich, które są nieznane lub zostały wykryte na tyle niedawno, że producent dziurawej aplikacji nie zdążył jeszcze przygotować odpowiedniej łaty. W takiej sytuacji dostawcom ochrony trudno jest zidentyfikować exploity wykorzystujące luki zero-day przy użyciu metod opartych na sygnaturach. Złożone exploity również mogą stosować szereg technik w celu obejścia technologii ochrony proaktywnej. Mimo że stosunkowo niewiele zagrożeń potrafi obejść tradycyjną ochronę, ogromne szkody, jakie mogą wyrządzić, uzasadniają wprowadzenie dodatkowej warstwy bezpieczeństwa – właśnie z tego powodu został stworzony moduł Automatycznego zapobiegania exploitom.

Jak działa Automatyczne zapobieganie exploitom

Technologia Automatyczne zapobieganie exploitom została stworzona w celu wykrywania szkodliwych programów, które wykorzystują luki w zabezpieczeniach oprogramowania. Jej rozwój opierał się na gruntownej analizie zachowania i funkcji najbardziej rozpowszechnionych exploitów. Badanie to pozwoliło zidentyfikować określone typy zachowania exploitów, pomagając odróżnić tego rodzaju szkodliwe oprogramowanie od innych niebezpiecznych, a także legalnych programów. Podczas tworzenia technologii uwzględniono również najczęściej atakowane programy.

Kontrola aplikacji potencjalnie podatnych na ataki

W technologii Automatyczne zapobieganie exploitom szczególną uwagę zwraca się na najczęściej atakowane programy, takie jak Java, Adobe Reader, Flash, Internet Explorer, Microsoft Office itd. Każda próba uruchomienia podejrzanych plików wykonywalnych lub kodu przez takie programy stanowi podstawę dla przeprowadzenia dodatkowej kontroli bezpieczeństwa. Takie zachowanie programu może być legalne – np. Adobe Reader może uruchomić inny plik wykonywalny w celu sprawdzenia, czy dostępne są aktualizacje. Jednak

niektóre cechy pliku wykonywalnego, jak również działania, które miały miejsce przed próbą jego uruchomienia, mogą wskazywać na szkodliwą aktywność.

Monitorowanie działań przed próbą uruchomienia

Informacje o aktywności programu sprzed próby uruchomienia szkodliwego kodu mogą być wykorzystane do zidentyfikowania szkodliwego oprogramowania. Technologia Automatyczne zapobieganie exploitom śledzi taką aktywność i identyfikuje źródło próby uruchomienia kodu. Źródło to może pochodzić z samego oprogramowania, ale może również wynikać z działań exploita. Dane dotyczące archetypowego zachowania exploita pomagają to wykryć, nawet w przypadku wykorzystania luki zero-day.

Śledzenie pochodzenia kodu

Niektóre exploity, zwłaszcza te wykorzystywane w atakach typu drive-by download (gdy exploit zostaje uruchomiony automatycznie w efekcie odwiedzenia szkodliwej strony internetowej), przechwytują szkodliwą funkcję z określonej strony internetowej, zanim zostanie wykonana. Technologia Automatyczne zapobieganie exploitom śledzi pochodzenie plików, potrafi zidentyfikować, która przeglądarka zainicjowała pobieranie, jak również określić zdalny adres WWW dla plików. Ponadto, w przypadku niektórych programów, Automatyczne zapobieganie exploitom może rozróżnić pliki stworzone za zgodą użytkownika od nieautoryzowanych nowych plików. Gdy ma miejsce próba uruchomienia podejrzanego kodu, informacje te pomagają określić działania exploita oraz zablokować go.

Zapobieganie wykorzystywaniu potencjalnych luk w zabezpieczeniach

W przypadku wielu programów i modułów oprogramowania, technologia Automatyczne zapobieganie exploitom wykorzysta moduł o nazwie *Wymuszone losowe generowanie układu przestrzeni adresowej.* Technologia ta jest również stosowana przez system operacyjny Windows (począwszy od wersji Windows Vista), jednak w przypadku Kaspersky Lab została rozszerzona na programy, które domyślnie nie obsługują tej metody. Dzięki temu, niektóre exploity nie będą mogły wykorzystać tej luki, ponieważ nie będą znały lokalizacji kodu w pamięci, która w innych przypadkach jest statyczna.

Dostępność

Technologia Automatyczne zapobieganie exploitom jest stosowana w szerokim wachlarzu produktów firmy Kaspersky Lab:

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

Korzyści

Technologia Automatyczne zapobieganie exploitom znacząco zmniejsza ryzyko, że urządzenie zostanie zainfekowane przez szeroko rozpowszechnione szkodliwe oprogramowanie lub stanie się celem ataku opartego na exploitach, nawet jeśli wykorzystana zostanie luka zero-day. W wewnętrznym teście technologia ta skutecznie zablokowała exploity wykorzystywane podczas ataków przeprowadzanych za pośrednictwem popularnych luk w zabezpieczeniach programów Adobe Flash Player, QuickTime Player, Adobe Reader i innych. Ponadto, ze względu na to, że Java stanowi najczęściej atakowane oprogramowanie, specjaliści z Kaspersky Lab znacząco udoskonalili możliwości technologii Automatyczne zapobieganie exploitom w zakresie wykrywania exploitów stworzonych dla tego programu. W 2013 r. technologia Automatyczne zapobieganie exploitom w produktach firmy Kaspersky Lab zablokowała ponad 6,4 mln ataków wymierzonych w ponad 1,1 mln użytkowników.

Jednym z najbardziej znamiennych przykładów efektywności omawianej technologii jest wykrycie proaktywne exploita wykorzystującego lukę zidentyfikowaną w komponencie Microsoft Graphics. Luka ta została wykryta w listopadzie 2013 r. i dotyczy systemów Windows, Microsoft Office oraz Microsoft Lync. Atakujący mógłby wykorzystać ją, przekonując użytkownika do podglądu lub otworzenia spreparowanej wiadomości e-mail, otworzenia specjalnie stworzonego pliku lub przeglądania specjalnie utworzonej zawartości internetowej. Atakujący, któremu udałoby się wykorzystać tę lukę, mógłby uzyskać te same uprawnienia co aktualny użytkownik. Innym dowodem wskazującym na skuteczność technologii Automatyczne zapobieganie exploitom był atak ukierunkowany Red October. Sam atak został wykryty w styczniu 2013 r., jednak niektóre z jego szkodliwych komponentów zostały zidentyfikowane przez technologie Automatyczne zapobieganie exploitom kilka miesięcy wcześniej niż po raz pierwszy usłyszeliśmy o tej cyberprzestępczej kampanii.

Celem Automatycznego zapobiegania exploitom są najbardziej złożone lub wcześniej nieznane niebezpieczne programy: szeroko rozpowszechnione szkodliwe obiekty zostaną zablokowane przez inne systemy bezpieczeństwa, takie jak Ochrona WWW, Ochrona plików, czy nawet filre antyspamowy. Dlatego też, technologia ta znacznie podnosi ogólne bezpieczeństwo użytkownika końcowego.