Technologia automatycznego zapobiegania exploitom

Podejście Kaspersky Lab do tematu bezpieczeństwa bazuje na wielu warstwach ochrony. Większość szkodliwych programów ma zostać zatrzymana w pierwszej warstwie – tzn. po detekcji przez metody oparte na analizie sygnatur zagrożeń. Niektóre złośliwe obiekty wymagają jednak specjalnego traktowania: musimy mieć pewność, że nawet jeśli ominą one jedną warstwę bezpieczeństwa, zostaną zatrzymane przez kolejną. Dla przykładu, jeżeli złożony złośliwy obiekt jest nowy, a jego sygnatura nie jest jeszcze znana, wciąż może on zostać wykryty i zablokowany przez usługę **Kaspersky Security Network**, która nieustannie zbiera od milionów użytkowników informacje o najnowszych cyberatakach. Kolejna warstwa ochrony to szeroka gama technologii proaktywnych, które analizują kod podejrzanych aplikacji. Nawet jeżeli aplikacji udało się uruchomić się na chronionym systemie, jej akcje zostaną namierzone, a niebezpieczna aktywność zostanie zablokowana przez moduł **Kontroli systemu**.

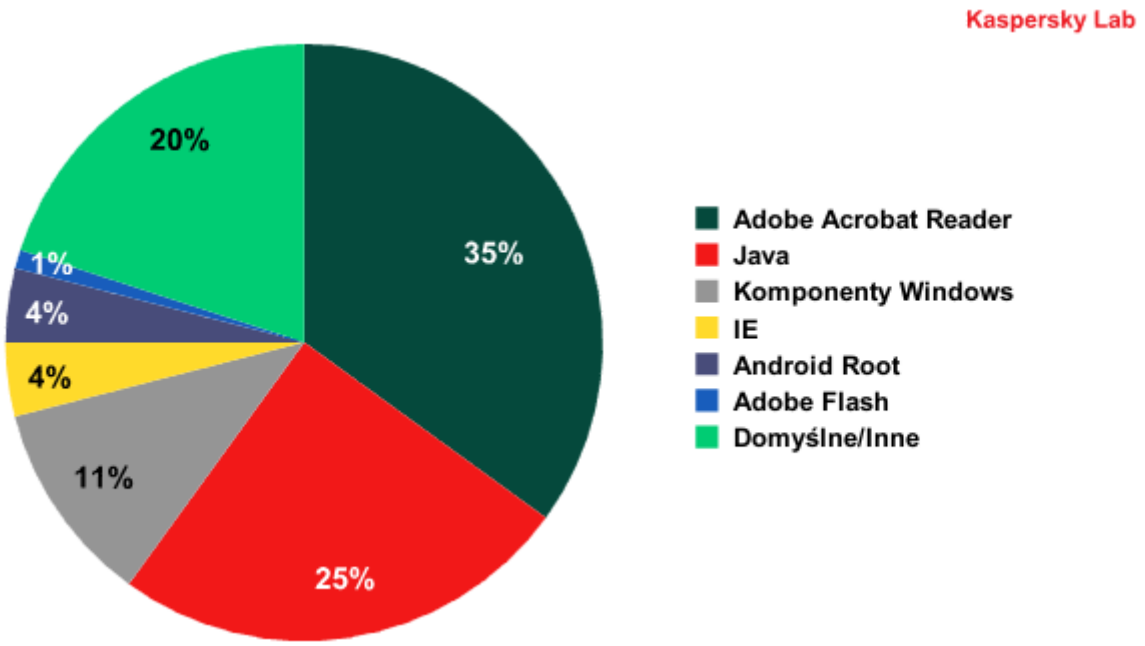
Istnieje jeszcze jeden obszar związany z cyberprzestępczością, który w naszym mniemaniu potrzebuje nowej, specjalnej warstwy ochrony: **exploity luk w popularnym oprogramowaniu**. Cyberprzestępcy robią użytek zarówno z dobrze znanych, jak i nowych (zero-day) luk w programach, takich jak: Adobe Flash, Adobe Reader, Java Runtime Environment. Również przeglądarki internetowe i rdzenne komponenty systemu operacyjnego Windows wykorzystywane są jako brama wiodąca szkodliwe oprogramowanie prosto do komputera użytkownika. Luki w zabezpieczeniach są nie tylko szeroko stosowane w złośliwym oprogramowaniu, ale stanowią również podstawę ataków ukierunkowanych, które mogą być trudne do wykrycia i zablokowania za pomocą konwencjonalnych metod ochrony. Nasza specjalistyczna warstwa ochrony, stworzona w oparciu o technologię o nazwie **Automatyczne zapobieganie exploitom** (Automatic Exploit Prevention – AEP), stanowi nowatorski i bardzo skuteczny sposób wykrywania nowych, nieznanych exploitów.

Typowe zachowanie exploitów

Celem każdego exploita jest wykorzystanie luk w oprogramowaniu, w celu uruchomienia różnego rodzaju złośliwego kodu. Aby infekcja z wykorzystaniem podatnego oprogramowania powiodła się, użytkownik musi zostać zwabiony na szkodliwą stronę internetową (lub na legalną stronę, do której podpięto złośliwy moduł) lub pobrać i uruchomić specjalnie spreparowany dokument (plik pakietu Office, PDF lub nawet obrazek, który wydaje się być totalnie nieszkodliwy). Złośliwe odsyłacze do zainfekowanych stron internetowych lub plików mogą być rozpowszechniane za pośrednictwem poczty elektronicznej, komunikatorów internetowych i sieci społecznościowych, a czasem pojawiają się nawet w wynikach wyszukiwania popularnych wyszukiwarek internetowych. Typowe ataki ukierunkowane rozpoczynają się często w momencie, gdy użytkownik otworzy specjalnie spreparowany załącznik e-mail, który często na pierwszy rzut oka wygląda zupełnie normalnie.

Najczęściej atakowane oprogramowanie

Prawie każdy program zawiera błędy, a niektóre z tych błędów mogą prowadzić do nieuprawnionego wykonania złośliwego kodu. Cyberprzestępcy jednak często specjalizują się w atakowaniu tylko popularnych programów, które są zainstalowane na większości komputerów – gwarantuje to dużą liczbę potencjalnych ofiar. Zgodnie ze statystykami Kaspersky Lab, w roku 2011 lista oprogramowania, najintensywniej atakowanego przez exploity, zawierała:



Z powyższego diagramu wynika, że aplikacja Adobe Reader była najczęściej atakowanym programem. Na drugiej pozycji uplasowało się środowisko Java Runtime Environment, a system operacyjny Windows zajmował trzecie miejsce z 11% zarejestrowanych ataków. Jedna piąta wszystkich ataków dotyczyła innego oprogramowania. Oznacza to, że do ataku ukierunkowanego cyberprzestępcy mogą wykorzystać lukę, która jest rzadko używana lub nawet nieznana. Z czasem lista najbardziej podatnego oprogramowania może się zmienić. Dla przykładu, w 2010 r. najczęściej atakowanym oprogramowaniem był pakiet biurowy Microsoft Office, Java i Adobe Flash. W pierwszym kwartale 2012 r. produkty Kaspersky Lab każdego miesiąca blokowały ponad milion plików zawierających exploity. Biorąc pod uwagę, że większość stron internetowych zawierających exploity była blokowana przez **Ochronę WWW**, niebezpieczeństwo tego aspektu działalności cyberprzestępców nie może być bagatelizowane.

Ogólne środki ochrony przed exploitami

Rozwiązanie bezpieczeństwa Kaspersky Internet Security wykorzystuje różne metody, aby pomóc w blokowaniu exploitów. Specjalne sygnatury, które pomagają wykryć szkodliwe pliki przed ich uruchomieniem, są dodawane do baz danych exploitów. **Ochrona proaktywna** i inne technologie zaawansowanego leczenia pozwalają używać funkcji, które mają wykrywać i blokować exploity po otwarciu podatnego pliku. Funkcja **Skanowania w poszukiwaniu luk** pomaga użytkownikom wyszukać podatne oprogramowanie i doradza, jak je zaktualizować. Oczywiście, wykonywanie regularnych aktualizacji komponentów systemu Windows i zainstalowanego oprogramowania jest najlepszym sposobem na uniknięcie większości exploitów.

© 1997-2012
Kaspersky Lab ZAO. Wszelkie prawa zastrzeżone.

W niektórych przypadkach ogólne techniki ochrony mogą być zawodne. Dotyczy to zwłaszcza luk zero-day – tych, które pozostają jeszcze nieznane lub zostały wykryte stosunkowo niedawno. W takich przypadkach producenci oprogramowania zabezpieczającego mają kłopot z rozpoznaniem exploitów, celujących w luki zero-day. Złożone exploity mogą również używać wielu technik omijania technologii ochrony proaktywnej. Nawet jeśli stosunkowo niewiele zagrożeń jest w stanie uciec przed metodami tradycyjnej ochrony, ogrom zniszczeń, jakie mogą poczynić, wymusza zastosowanie dodatkowej warstwy ochronnej – i to jest zadanie dla technologii **Automatycznego zapobiegania exploitom**.

W jaki sposób działa Automatyczne zapobieganie exploitom?

Technologia Automatycznego zapobiegania exploitom została zaprojektowana z myślą o szkodliwym oprogramowaniu, które wykorzystuje podatności w aplikacjach. Jej rozwój rozpoczął się od gruntownej analizy zachowania i cech najbardziej rozpowszechnionych exploitów. Badania te pozwoliły na zidentyfikowanie określonych typów zachowania exploitów, które pomagają odróżnić ten rodzaj złośliwego oprogramowania od innych szkodliwych programów i legalnych aplikacji. Poza tym, w trakcie rozwoju tej technologii, można było wziąć pod uwagę najczęściej atakowane programy. W wyniku tych działań najnowsze wersje Kaspersky Internet Security i Kaspersky Anti-Virus będą zawierały technologię Automatycznego zapobiegania exploitom jako dodatek do standardowego modułu Kontroli systemu.

Kontrolowanie potencjalnie podatnych aplikacji

Technologia Automatycznego zapobiegania exploitom zwraca szczególną uwagę na najczęściej atakowane programy, takie jak: Adobe Reader, Internet Explorer, Microsoft Office itp. Wszelkie próby tych programów, podejmowane w celu uruchomienia podejrzanych plików wykonywalnych lub szkodliwego kodu, są punktem wyjścia do przeprowadzenia dodatkowych kontroli bezpieczeństwa. Takie działania nie do końca muszą być jawnie szkodliwe – na przykład Adobe Reader może uruchomić inny plik wykonywalny, aby ten zaczął szukać uaktualnień. Ale pewne cechy pliku wykonywalnego, a także działania, które miały miejsce przed próbą uruchomienia pliku, mogą wskazywać na jego szkodliwą naturę.

Monitorowanie działań przed próbą uruchomienia

Informacje o aktywności programu przed próbą uruchomienia podejrzanego kodu mogą być również używane do identyfikacji złośliwego oprogramowania. Technologia Automatycznego zapobiegania exploitom śledzi tę aktywność i odkrywa źródło próbujące uruchomić kod. Źródło może pochodzić z samego oprogramowania, ale może być również wynikiem działania exploita. Dane dotyczące najbardziej typowego zachowania exploitów pomagają wykryć nawet przypadki prób wykorzystania luk zero-day.

Śledzenie pochodzenia kodu

Określone typy exploitów, zwłaszcza te używane w atakach **drive-by download** (sytuacja, w której exploit zostaje uruchomiony w trakcie odwiedzania złośliwej strony internetowej), przechwytują ładunek z podejrzanych stron internetowych przed jego uruchomieniem. Technologia Automatycznego zapobiegania exploitom śledzi źródła plików, zna dokładne informacje o przeglądarce, która zainicjowała pobieranie i zdalny adres internetowy szkodliwych plików. Dodatkowo, w niektórych programach technologia Automatycznego zapobiegania exploitom rozróżnia pliki utworzone za zgodą użytkownika i nieautoryzowane nowe pliki. Kiedy nastąpi próba wykonania szkodliwego kodu, te informacje pomagają określić działania exploita i natychmiast je zablokować.

© 1997-2012
Kaspersky Lab ZAO. Wszelkie prawa zastrzeżone.

Uniemożliwienie wykorzystywania potencjalnych luk

Dla wielu programów i modułów programowych technologia Automatycznego zapobiegania exploitom używa trybu zwanego „wymuszoną randomizacją warstwy przestrzeni adresowej” (Forced ASLR). Technologia **ASLR** jest również stosowana w systemach operacyjnych Windows (poczynając od Microsoft Windows Vista), lecz w produktach Kaspersky Lab została ona rozszerzona na wiele programów. W rezultacie, niektóre exploity nie będą w stanie wykorzystać danej luki, ponieważ lokalizacja złośliwego kodu w pamięci (normalnie statyczna, a teraz dynamiczna) nie będzie dla nich znana.

Dostępność

Technologia Automatycznego zapobiegania exploitom jest dostępna w linii 2013 produktów Kaspersky Internet Security i Kaspersky Anti-Virus. W produktach tych technologia AEP jest aktywowana przy użyciu domyślnych ustawień, ale może zostać wyłączona oddzielnie lub wraz z całym modułem Kontroli systemu, który śledzi ogólne zachowanie programów w systemie. Domyślnie, technologia Automatycznego zapobiegania exploitom blokuje wykonanie jakiegokolwiek podejrzanego kodu: metody wprowadzane przez tę nową technologię sprawiają, że prawdopodobieństwo wystąpienia fałszywych alarmów są znikome. Funkcja AEP może zostać uruchomiona również w trybie interaktywnym.

Korzyści

Technologia Automatycznego zapobiegania exploitom znacznie zmniejsza szanse na zarażenie systemu powszechnym złośliwym oprogramowaniem lub stania się ofiarą ataku ukierunkowanego korzystającego z exploitów, nawet w przypadku luk zero-day. Podczas wewnętrznych testów, technologia AEP skutecznie blokowała exploity wykorzystujące luki w powszechnie wykorzystywanych aplikacjach, takich jak: Adobe Flash Player, QuickTime Player, Adobe Reader, Java itd. Jednym z najbardziej godnych uwagi przykładów skuteczności tej technologii jest wykrycie exploita, który wykorzystuje jedną z ostatnich luk znalezionych w Windows Media Player. Podatność ta została wykryta w styczniu 2012 r. i dotyczyła wszystkich systemów operacyjnych Windows, począwszy od Windows XP. Pozwalała na zdalne wykonanie kodu przy użyciu specjalnie spreparowanego pliku .MIDI – pliku muzycznego, który zdawałby się być kompletnie nieszkodliwy.

Technologia Automatycznego zapobiegania exploitom powstała z myślą o wykrywaniu najbardziej skomplikowanych lub nieznanych wcześniej exploitów. Typowe szkodliwe obiekty będą blokowane przez inne systemy bezpieczeństwa, takie jak: **Ochrona WWW**, **Ochrona plików** lub filtr **Anti-Spam**. Automatyczne zapobieganie exploitom znacznie zwiększa ogólne bezpieczeństwo użytkownika końcowego.

© 1997-2012
Kaspersky Lab ZAO. Wszelkie prawa zastrzeżone.