**Czy istnieje ochrona przed szkodnikami wykorzystującymi luki w Javie?**

**W ciągu minionych sześciu miesięcy dwa miliony użytkowników stanowiło cel cyberataków z wykorzystaniem szkodliwych programów infekujących poprzez luki w Javie.**

Eksperci z Kaspersky Lab przeprowadzili badanie dotyczące jednej z najpopularniejszych metod atakowania komputerów – wykorzystywania pakietów exploitów, czyli szkodliwych programów infekujących poprzez luki w zabezpieczeniach legalnego oprogramowania. Według badaczy ulubionym narzędziem cyberprzestępców są obecnie exploity Javy. Nie jest to żadną niespodzianką, biorąc pod uwagę fakt, że tylko w ciągu ostatnich 12 miesięcy wykryto ponad 161 luk w JRE (Java Runtime Environment). Od marca do sierpnia 2013 r. chmura Kaspersky Security Network zarejestrowała ataki wykorzystujące exploity Javy, których celem było ponad 2 miliony użytkowników.

Podczas badania eksperci z Kaspersky Lab próbowali ustalić, w jaki sposób infekowane były komputery przy użyciu pakietu exploitów BlackHole – jednego z najpopularniejszych narzędzi cyberprzestępców (obok takich pakietów jak Nuclear Pack, Styx Pack oraz Sakura). BlackHole zawiera exploity wykorzystujące luki w takich aplikacjach jak Adobe Reader, Adobe Flash Player, Oracle Java oraz innym popularnym oprogramowaniu. Ponieważ działanie wszystkich pakietów exploitów opiera się na podobnym schemacie, eksperci z Kaspersky Lab wybrali trzy exploity Javy z zestawu BlackHole, aby przedstawić zasady działania takich pakietów.

Na przykładzie BlackHole pokazano również interakcję komponentów ochrony ze szkodliwym kodem na różnych etapach, łącznie z etapem wywoływania exploitów wykorzystujących określone luki w zabezpieczeniach:

blokowanie strony startowej pakietu exploitów (tj. pierwszej strony pakietu exploitów po tym, jak użytkownik zostanie przekierowany z legalnej witryny);

wykrywanie przy użyciu modułu ochrony plików (jeżeli mimo to użytkownik trafi na stronę startową pakietu exploitów);

wykrywanie exploitów w oparciu o sygnatury (w przypadku gdyby rozwiązanie bezpieczeństwa nie wykryło strony startowej pakietu exploitów);

proaktywne wykrywanie exploitów (przydatne, jeżeli żaden komponent ochrony opartej na sygnaturach nie wykryje niczego szkodliwego podczas skanowania zawartości pakietu exploitów i exploit zdoła się uruchomić);

wykrywanie pobranego szkodliwego oprogramowania (jeżeli exploit uniknie wykrycia, próbuje pobrać szkodliwą funkcję i uruchomić ją na komputerze ofiary).

*„Dzisiaj jeżeli cyberprzestępca chce zainfekować komputery, powiedzmy modyfikacją trojana ZeuS, musi tylko kupić stworzony wcześniej pakiet exploitów, skonfigurować go i zwabić możliwie jak największą liczbę potencjalnych ofiar na jego stronę docelową. Problem ‘czarnych dziur’ nadal jest aktualny mimo badań nad mechanizmem infekcji pakietów exploitów oraz wszechstronnych rozwiązań oferowanych przez producentów ochrony. W przypadku Javy producent oprogramowania dość szybko reaguje na nowo wykryte luki i publikuje odpowiednie łaty. Jednak użytkownicy końcowi zwykle nie śpieszą się z instalowaniem aktualizacji, a cyberprzestępcy przejmują inicjatywę, tworząc nowe szkodliwe programy wykorzystujące znane braki w zabezpieczeniach”* – powiedział Wiaczesław Zakorzewski, szef grupy zajmującej się badaniami dotyczącymi luk w zabezpieczeniach, Kaspersky Lab.

Jak dotąd pakiety exploitów zapewniały cyberprzestępcom niezwykle skuteczny sposób infekowania komputerów, w przypadku gdy nie zainstalowano na nich żadnego systemu bezpieczeństwa i istnieje co najmniej jeden popularny pakiet oprogramowania z niezałataną luką. Nie jest żadną niespodzianką, że infekcje z wykorzystaniem pakietów exploitów stanowią popularną metodę wśród cyberprzestępców: jest ona bardzo trudna do wykrycia dla niedoświadczonego użytkownika, szczególnie gdy nie korzysta on z żadnego rozwiązania bezpieczeństwa.

Proces rozpoczyna się od przekierowania użytkownika na stronę docelową exploitów. W tym celu cyberprzestępcy wykorzystują szeroką gamę metod, w tym wiadomości spamowe zawierające odsyłacze do takich witryn. Jednak najgroźniejsza sytuacja ma miejsce wtedy, gdy cyberprzestępcy włamią się na legalne strony i wstrzykną do nich swój szkodliwy kod. W takich przypadkach wystarczy, że użytkownik odwiedzi znajomą stronę, a zostanie przeprowadzony na niego atak drive-by i pakiet exploitów rozpocznie swoje „podstępne” działanie. Cyberprzestępcy mogą również wykorzystać legalne systemy reklamowe i banery prowadzące na szkodliwe strony.

Jedynym pewnym sposobem zapobiegnięcia atakowi jest dopilnowanie, aby na komputerze nie zostało zainstalowane żadne oprogramowanie, którego wymaga pakiet exploitów. Jak tylko użytkownik odwiedzi stronę docelową, cyberprzestępcy pobiorą informacje z komputera ofiary, w tym dotyczące wersji systemu operacyjnego, przeglądarki internetowej i wszystkich zainstalowanych wtyczek, konfiguracji lokalnych języków itd. Jeżeli cyberprzestępcy zauważą, że istnieje wymagana kombinacja – a w przypadku luk wykrytych w popularnych pakietach, takich jak Adobe Reader, Adobe Flash Player oraz Oracle Java, taka kombinacja zwykle istnieje – wtedy zostaną wybrane odpowiednie expoity w celu przeprowadzenia ataku na dany komputer.

Kolejnym powodem, dla którego cyberprzestępcy mogą zaprzestać ataku, jest próba uniknięcia wykrycia przez ekspertów z firm antywirusowych lub innych badaczy. Na przykład, cyberprzestępcy mogą umieścić na „czarnej liście” adresy IP wykorzystywane przez firmy badawcze, zablokować uruchamianie exploitów na maszynach wirtualnych itd.

Więcej informacji na temat ataków wykorzystujących luki w popularnym oprogramowaniu znajduje się w serwisie [SecureList.pl](http://www.securelist.pl) prowadzonym przez Kaspersky Lab.

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>.