**Kaspersky Lab wykrywa i pomaga załatać nową lukę w Adobe Flash Player**

**System wykrywania heurystycznego wbudowany w produkty Kaspersky Lab zablokował ataki prowadzone z użyciem nieznanego dotychczas błędu w zabezpieczeniach aplikacji Adobe Flash Player.**

Badacze z Kaspersky Lab zidentyfikowali lukę służącą do przeprowadzania ataków w ramach legalnej strony rządowej, która pierwotnie powstała w celu gromadzenia skarg obywateli w jednym z krajów Bliskiego Wschodu.

W połowie kwietnia, podczas analizy danych pochodzących z chmury [Kaspersky Security Network](http://www.kaspersky.pl/images/news/klp_kaspersky_security_network.pdf), eksperci z Kaspersky Lab wyryli nieznany dotychczas atak. Po szczegółowym badaniu okazało się, że wykorzystuje on nieznaną wcześniej lukę w popularnym oprogramowaniu Adobe Flash Player, a dokładniej w module Pixel Plender wykorzystywanym do przetwarzania filmów i zdjęć.

Dalsza analiza wykazała, że ataki były przeprowadzane z użyciem strony stworzonej w 2011 r. przez syryjskie Ministerstwo Sprawiedliwości w celu umożliwienia obywatelom składania zażaleń dotyczących naruszeń prawa. Eksperci z Kaspersky Lab podejrzewają, że atak został zaprojektowany w celu uderzenia w syryjskich decydentów skarżących się na rząd.

Eksperci z Kaspersky Lab wykryli łącznie dwa rodzaje ataków, które wykorzystywały inny kod.

„Pierwszy atak był raczej prymitywny, natomiast drugi wykorzystywał wtyczkę Cisco MeetingPlace Express Add-In, która standardowo służy do pracy grupowej, a dokładniej do wspólnego przeglądania dokumentów i zdjęć. Wtyczka ta jest całkowicie legalna, jednak atakujący wykorzystali ją jako narzędzie szpiegowskie. Co więcej, wykryliśmy, że atak ten był skuteczny tylko na konkretnej wersji Flash Playera i wtyczki Cisco, co może oznaczać, że cyberprzestępcy celowali w bardzo wąskie grono ofiar”, tłumaczy **Wiaczesław Zakorzewski**, menedżer grupy odpowiedzialnej za badania nad lukami w zabezpieczeniach, Kaspersky Lab.

Natychmiast po wykryciu ataku specjaliści z Kaspersky Lab skontaktowali się z przedstawicielami Adobe, by poinformować ich o nieznanej luce. Po dokonaniu analizy informacji dostarczonych przez Kaspersky Lab eksperci z Adobe potwierdzili istnienie nieznanej luki ([CVE-2014-0515](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-0515)) i przygotowali usuwającą ją łatę, która jest już dostępna do pobrania na stronie Adobe.

„Mimo że zaobserwowaliśmy ograniczoną liczbę ataków wykorzystujących tę nieznaną wcześniej lukę, zalecamy wszystkim użytkownikom jak najszybsze uaktualnienie oprogramowania Adobe Flash Player. Istnieje prawdopodobieństwo, że po upublicznieniu informacji o luce cyberprzestępcy będą próbowali przygotować modyfikacje wykorzystujących ją ataków. Uważamy, że stopień zagrożenia związany z tą luką jest dość wysoki, szczególnie biorąc pod uwagę popularność aplikacji Flash Player na całym świecie oraz to, że użytkownicy często odkładają uaktualnianie systemów i aplikacji na później” – dodaje **Wiaczesław Zakorzewski**.

**Informacje o systemie wykrywania heurystycznego**

System wykrywania heurystycznego stanowi element silnika antywirusowego wykorzystywanego w produktach Kaspersky Lab przeznaczonych dla użytkowników domowych i firm, takich jak Kaspersky Anti-Virus, Kaspersky Internet Security czy Kaspersky Endpoint Security for Business. System ten, podobnie jak tradycyjne oprogramowanie antywirusowe, wykorzystuje sygnatury do wykrywania szkodliwego oprogramowania. Jednak, podczas gdy technologia antywirusowa zazwyczaj wymaga oddzielnej sygnatury dla każdego szkodliwego programu – niezależnie od ich podobieństwa, wykrywanie heurystyczne pozwala na objęcie całej gamy zagrożeń przy użyciu jednego wpisu w bazach danych. Jest to możliwe dzięki zastosowaniu specjalnych sygnatur, które wykrywają zagrożenia w oparciu o zestaw parametrów. Sygnatura, która pozwoliła na wykrycie ataku przeprowadzanego przy użyciu nieznanej luki w aplikacji Adobe Flash Player i ochroniła użytkowników została dodana do baz w styczniu 2014 r.

Co więcej, podczas szczegółowych badań okazało się, że ataki wykorzystujące tę lukę są również skutecznie blokowane proaktywnie przez inną technologię Kaspersky Lab – [Automatyczne zapobieganie expliotom](http://www.kaspersky.pl/images/news/klp_automatyczne_zapobieganie_exploitom.pdf). W listopadzie 2013 r. ten system służący do ochrony przed nieznanymi atakami skutecznie zablokował szkodliwą aktywność korzystającą z luki w oprogramowaniu [Microsoft Office](http://www.kaspersky.pl/about.html?s=news_warnings&amp;amp;cat=4&amp;amp;newsid=2143). Pod koniec 2012 r. ta sama technologia zablokowała kilka szkodliwych modułów, które – jak się później okazało – stanowiły część kampanii cyberszpiegowskiej [Red October](http://www.kaspersky.pl/about.html?s=news_warnings&amp;amp;cat=4&amp;amp;newsid=1857) wykrytej w styczniu 2013 r. przez badaczy z 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>.