Czy zwykłe przeglądanie plików PDF może być niebezpieczne? Jak najbardziej. Dowiedz się w jaki sposób cyberprzestępcy wykorzystują nasze największe słabości i co możesz na to poradzić.

O groźnie wyglądającej „dziurze" w funkcjach programów Adobe Reader oraz FoxIt Reader powiadomił na swoim blogu Didier Stevens, belgijski profesjonalista pracujący w dziedzinie bezpieczeństwa IT. Problemem zainteresowały się również duże media, jak choćby CNET News.

Pięta achillesowa PDF
Stevens ostrzegł, że otwieranie programów poprzez linki zawarte w plikach PDF może prowadzić do nieumyślnego uruchomienia złośliwego oprogramowania i zarażania nim docelowo komputerów użytkowników Internetu. Na straty narażone są osoby, które klikają w plikach PDF linki odsyłające do różnych zasobów, np. innych, niepewnych plików PDF znajdujących się w Internecie.

„W Adobe Reader użytkownik otrzymuje w specjalnym okienku ostrzeżenie z zapytaniem o podjęcie następnej akcji – mówi Stevens. Pozwala mi to utrzymywać częściową kontrolę nad następnymi działaniami programu. FoxIt Reader nie wyświetla natomiast żadnego ostrzeżenia i po kliknięciu w link, akcja zostaje rozpoczęta bez jakiejkolwiek zgody ze strony użytkownika."
Co więcej, należy dodać, że cyberprzestępcy mieli możliwość częściowej zmiany tekstu samego okna dialogowego na taki, który zachęci nieświadomą niczego osobę do uruchomienia złośliwego oprogramowania. W wyniku tego, również wszystkie pozostałe pliki PDF na naszym dysku mogą ulec zarażeniu. Stąd dzieli nas już tylko krok od przejęcia przez cyberprzestępcę kontroli nad naszym komputerem.

„W tym przypadku nie ma miejsca wykorzystywanie luki w samym kodzie programów, lecz obejście zabezpieczeń w zupełnie legalny sposób. Wyłączenie JavaScript nic więc nie pomoże" – kontynuuje Stevens.

Co na to Adobe i FoxIt?
Jak informuje serwis ZDNet, Didier Stevens powiadomił o swoim odkryciu ekspertów z Adobe oraz FoxIt, ci natomiast niezwłocznie przystąpili to pracy nad zminimalizowaniem ryzyka zagrożeń.
W oświadczeniu prasowym wydanym przez Adobe czytamy: „…Wiadomość ostrzegawcza wyświetlana w programach Adobe Reader oraz Adobe Acrobat zawiera wyraźną wzmiankę o tym, aby otwierać tylko takie pliki, co do których mamy pewność, że pochodzą z zaufanego źródła. Adobe podchodzi bardzo poważnie do kwestii bezpieczeństwa produktów oraz technologii; dokładamy starań, aby administratorzy oraz użytkownicy końcowi mogli bardziej skutecznie zarządzać oraz konfigurować opcje taki sposób, aby zmniejszyć potencjalne ryzyko użytkowania naszych programów."
Natomiast FoxIt ujął to w taki sposób: „FoxIt bardzo poważnie podchodzi do spraw bezpieczeństwa. Obecnie skupiamy się na ustaleniu przyczyny problemu oraz pracujemy nad możliwymi rozwiązaniami poprawiającymi bezpieczeństwo. W ciągu ostatnich 24 godzin wypracowaliśmy pewne rozwiązania. Zaktualizowana wersja FoxIt Reader będzie dostępna do pobrania w ciągu następnych 72 godzin."

Czy jest ratunek?
Sprawę komentuje Tomasz Zamarlik, specjalista ds. oprogramowania antywirusowego z firmy **G Data Software**: „Jest to problem, którego nie można łatwo naprawić, ponieważ ma on więcej wspólnego z wykorzystywaniem ludzkiej łatwowierności, niż z błędami w samym kodzie programów do czytania plików PDF. Bardzo prawdopodobne, że przyszłe wersje oprogramowania będą zawierać mocniejsze ostrzeżenie o konsekwencjach otwierania obcych programów bądź plików. Na chwilę obecną można samemu ręcznie wyłączyć opcję otwierania z poziomu pliku PDF aplikacji zewnętrznych innych niż format PDF. Zawsze wypadało by jednak mieć ratunkową poduszkę powietrzną w postaci zainstalowanego oprogramowania antywirusowego."

Someday Interactive