Cyberdefence 24

aut. Tomasz Fastyn 04.04.2017

ZHAKOWANA STRONA DAESH ROZSIEWAŁA ZŁOŚLIWE OPROGRAMOWANIE

Agencja informacyjna Amaq, która służy do rozpowszechniania propagandy Państwa Islamskiego, została przejęta przez hakerów powiązanych ze słynną grupą Anonymous. Hakerzy ingerując w kod strony zaimplementowali złośliwy plik aktualizacji wtyczki Flash, który mógł zostać nieświadomie pobrany przez odwiedzających.

Ataki hakerów na strony i media powiązane z Daesh nie są nowością. Tylko w zeszłym roku doszło do wielu włamań na fora przewidziane do kontaktów pomiędzy dżihadystami. Walkę z ISIS w cyberprzestrzeni prowadzą także Stany Zjednoczone, które starają się zamknąć jak najwięcej witryn powiązanych z ekstremistami.

Sposób działania hakerów z grupy Anonymous, którzy wzięli odpowiedzialność za atak na stronę Amaq, można uznać za dosyć rzadki przypadek. Celem włamania nie było jedynie wyłączenie strony czy zablokowanie przepływu informacji pomiędzy komórkami ISIS, ale próba włamania na urządzenia osób odwiedzających witrynę. Fakt włamania na stronę Amaq przekazali terroryści na jednej z grup tematycznych utworzonych dzięki aplikacji Telegram. Sprawę później potwierdziły osoby powiązane z agencją informacyjną.

Czytaj też: Wiceprezes Trend Micro: Atak na KNF częścią zaawansowanej kampanii hakerskiej [WYWIAD]

Złośliwe oprogramowanie we Flashu było dostarczane za pomocą sprawdzonej przez hakerów metody. Po wejściu na stronę Amaq pojawiał się komunikat o starej wersji wtyczki Adobe Flash Player. Instalacja była pobierana automatycznie po kliknięciu przez odwiedzającego w przycisk ok, na pop-upie.

Raphael Gluck, który jako pierwszy podał informację, opublikował na swoim profilu Twitter zrzut ekranu wykonany podczas odwiedzania strony. Widać na nim, że przeglądarka Chrome zwróciła uwagę na pobierany plik, który może stanowić zagrożenie dla użytkownika. Nie wiadomo, czy inne przeglądarki również traktowały plik jako niebezpieczny. Według niepotwierdzonych informacji, co najmniej 600 osób ściągnęło kod wykonywalny.

Plik pobierany ze strony Amaq, był tzw. dropperem, który dopiero po zainstalowaniu pobierał złośliwe oprogramowanie na urządzenia ofiary. Według jednego z ekspertów, właściwym wirusem był Bladabindi, znany także jako NJRat.