Zdaniem ekspertów, którzy odkryli następcę Stuxneta, czyli trojana Duqu został on zaprojektowany specjalnie do kradzieży danych firmowych. Choć nie ustalono jeszcze dokładnie jego pochodzenia oraz wszystkich efektów działania, jedno jest pewne: celem Duqu są komputery z systemem Windows. System IPS w urządzeniach gateProtect zapobiegają penetracji sieci przez tego trojana udowadniając tym samym, że ochrona przed nim jest możliwa.

Duqu zachowuje się jak typowy trojan bot netowy. Po infekcji komputera Duqu szyfruje informacje i wysyła je do serwera zarządzającego całą operacją. Może również na zainfekowanym komputerze zainstalować keyloggera, czyli program zapisujący wszystkie znaki wpisywane z klawiatury. Służy to najczęściej kradzieży haseł dostępowych, które mogą zostać wykorzystane przez cyberprzestępców do przygotowania ataku informatycznego na firmę.

Urządzenia gateProtect to kompleksowe systemy zapobiegania włamaniom, zawierające najnowsze sygnatury, zaprojektowane specjalnie aby blokować tego typu intruzów. W rezultacie zapora gateProtect jest w stanie powstrzymać nastepcę Stuxneta i wykonywaną przez niego kradzież danych. Blokuje również jego dostęp do Internetu zapobiegając tym samym wyciekowi danych.

Jak mówi Elżbieta Kasprzyk, channel manager rozwiązań gateProtect „Zagrożenia związane z Internetem są coraz bardziej zaawansowane technologicznie. Trojan Duqu jest tego najlepszym przykładem. Ataki cyberprzestępców, kradzież, niszczenie danych, wszystko to może zagrozić ciągłości działania biznesu. Dlatego też tak ważne jest wdrażanie przez firmy potężnych mechanizmów obronnych, takich jak urządzenia gateProtect, obejmujące również systemy IPS”.

Mediarecovery