Zamaskowany w elektronicznej pocztówce nowy szkodnik Trj.Downloader.Fakealert.FA (G Data Software) lub Worm.Win32.Kucirc (Microsoft) oprócz destabilizacji pracy systemu generuje fałszywe komunikaty o infekcjach. Celem cyberprzestępców jest zastraszenie i sprowokowanie ofiary do podania ważnych informacji oraz kupna fałszywego antywirusa.

Cyberprzestępcy dołączając groźne pliki do elektronicznych pocztówek wracają do sprawdzonych metod rozpowszechniania malware. W minionym miesiącu hakerzy dzięki tej metodzie pozyskali dane wielu użytkowników sieci. Jednym z nowych zagrożeń obecnych w sieci jest zamaskowany w elektronicznej pocztówce, bardzo agresywny w swoim działaniu trojan **Trj.Downloader.Fakealert.FA**. Jego destrukcyjne działanie oraz liczne komunikaty o infekcjach wywierają na użytkowniku ogromną presję podania danych i wykonania przelewu na konto cyberprzestępcy. Tuż po wtargnięciu do systemu operacyjnego szkodnik w celu pobrania kolejnych wirusów nawiązuje połączenia z amerykańskimi serwerami. Dodatkowo uruchamia własną przeglądarkę www i wyświetlając strony z teksańskich serwerów wyłudza dane personalne oraz nakłania do zakupu fałszywego antywirusa. Ponadto szkodnik podtrzymując swoje rozpoczęte wątki uniemożliwia uruchomienie pozostałych programów zainstalowanych w komputerze. W menadżerze zadań do widoku uruchomionych procesów dodaje kolumnę, w której wybrane procesy oznacza jako „infected”.

Źródło: G Data Software