Znaleziono niezwykły szkodliwy kod

22 marca 2012

Specjaliści odkryli niezwykle rzadki, możliwe że jedyny w swoim rodzaju, szkodliwy kod, który nie pozostawia na zarażonym komputerze żadnych plików. Odkrycia dokonali eksperci z Kaspersky Lab, którzy zauważyli na rosyjskich witrynach kod atakujący dziurę w Javie. Kod ładuje się bezpośrednio do pamięci komputera i nie pozostawia na dysku twardym żadnych plików. Szkodliwy kod JavaScript korzysta z elementu iFrame i wstrzykuje szyfrowaną bibliotekę (.dll) bezpośrednio do procesu Javaw.exe.

Wydaje się, że kod ma na celu wyłączenie mechanizmu User Account Control (UAC) oraz umożliwienie komunikowania się serwera cyberprzestępców z komputerem ofiary i ewentualnie wgranie nań trojana Lurk, wyspecjalizowanego w kradzieży danych.

– Z naszych analiz protokołu komunikacyjnego używanego przez Lurk wynika, że w ciągu ostatnich miesięcy serwery przestępców przetworzyły do 300 000 zapytań od zainfekowanych komputerów – stwierdził Siergiej Gołowanow z Kaspersky Lab.

Opracowanie: Mariusz Błoński
Na podstawie: TechWorld
Źródło: Kopalnia Wiedzy