Grum wyłączony

23 lipca 2012
Udało się zamknąć botnet, który odpowiadał za rozsyłanie 18% światowego spamu. Serwery botnetu Grum znajdowały się głównie w Panamie, Rosji i na Ukrainie.

Botnetowi wojnę wydały firma FireEye i serwis SpamHaus, którym we współpracy z dostawcami internetu udało się wyłączyć serwery.

Najpierw wyłączono serwer kontrolny w Holandii, a następnie w Panamie. Gdy eksperci sądzili, że wystarczy jeszcze wyłączyć serwery w Rosji okazało się, że przestępcy zauważyli co się dzieje i błyskawicznie założyli nowe serwery na Ukrainie. Kraj ten tradycyjnie jest bezpieczną przystanią dla tego typu przedsięwzięć.

Jednak tym razem dzięki współpracy z ekspertami z wielu krajów udało się wyłączyć również serwery na wschodzie.

Specjaliści oceniają, że jeszcze ponad 20 000 pecetów jest połączonych w botnet, jednak przestępcy utracili nad nimi kontrolę.

„Nie ma już bezpiecznych miejsc. Serwery kontrolne większości botnetów, które dotychczas znajdowały się w USA i Europie, zostały poprzenoszone przez ich twórców do krajów takich jak Ukraina, Rosja czy Panama, w nadziei, że będą tam bezpieczne. Pokazaliśmy im, że nie mają racji” – stwierdził Atif Mushtaq z FireEye.

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