ZLIKWIDOWANA SIEĆ BOTNET INFEKUJĄCA KOMPUTERY NA CAŁYM ŚWIECIE

Data publikacji 15.07.2014

Policjanci z Biura Służby Kryminalnej Komendy Głównej Policji wzięli udział w operacji pod nazwą Shylock. Międzynarodowe działania koordynowane były przez brytyjską Policję, których wynikiem było wyłączenie serwerów stanowiących rdzeń sieci BotNet, dzięki której złośliwe oprogramowanie Shylock infekowało podłączone do Internetu komputery.

W dniach 08 – 09 lipca 2014r. miała miejsce międzynarodowa operacja, wymierzona w sieć BotNet, za pośrednictwem której rozpowszechniano złośliwe oprogramowanie o nazwie Shylock. Działania polegały na wyłączeniu serwerów rozmieszczonych na całym świecie, tworzących system zarządzania siecią BotNet (command and control system), a także przejęciu kontroli nad domenami, wykorzystywanymi przez złośliwe oprogramowanie do komunikacji między zainfekowanymi komputerami.

Operacja koordynowana była przez Brytyjską National Crime Agency (NCA). Udział w niej wzięli przedstawiciele organów ścigania ze Stanów Zjednoczonych (FBI), Europejskiego Urzędu Policji (Europolu), Włoszech, Holandii i Turcji, przy współpracy z partnerami z Polski, Niemiec oraz Francji.

Do współpracy zaproszono również przedstawicieli reprezentujących sektor prywatny. Z ramienia polskiej Policji w działaniach brali udział funkcjonariusze Wydziału Wsparcia Zwalczania Cyberprzestępczości Biura Służby Kryminalnej KGP.

Wynikiem operacji było wyłączenie serwerów stanowiących rdzeń sieci BotNet, dzięki której Shylock mógł być rozpowszechniany i infekował działające w sieci Internet komputery. Dodatkowo odkryto wcześniej nieznane elementy wskazanej infrastruktury, dzięki czemu można było podjąć niezbędne kroki do jak najszybszego wyłączenia kolejnych serwerów.

Na terenie Polski został ujawniony jeden serwer, stanowiący część opisanej sieci BotNet. Przy współpracy policjantów z Biura Służby Kryminalnej KGP zwalczających cyberprzestępczość z właścicielem serwera, został on wyłączony i nie stanowi już zagrożenia dla Internautów.

Shylock to trojan, który został wykryty po raz pierwszy w 2011 r. Działa poprzez lukę w przeglądarkach internetowych, co pozwala na przejęcie kontroli nad zainfekowanym komputerem. Blokuje wykrywanie go przez powszechne programy antywirusowe, a następnie wykrada wrażliwe dane ofiary – w szczególności dane wykorzystywane do logowania do portali bankowych.

(BSK KGP)