Cienka granica między cyberprzestępczością a cyberwojną

15 listopada 2012

Gdy w 2008 roku rozpoczęła się wojna między Gruzją a Rosją, Abchazją i Osetią Południową pole walki miało znacznie większy zasięg niż ten pokazywany w telewizji, który objął kilka regionów. Istotnym epizodem tej wojny był przypisywany Rosjanom atak przeprowadzony w Internecie.

Przeprowadzony atak internetowy spowodował paraliż oficjalnych gruzińskich serwisów, co doprowadziło do blokady informacyjnej. Przez nią Gruzja nie była w stanie zaprezentować światu swojego stanowiska w sprawie wojny, przez co do mediów trafiały jedynie rosyjskie relacje. Co więcej, wraz z rozpoczęciem walk na stronach rosyjskich pojawiły informacje zawierające narzędzie i instrukcje pozwalające na przyłączenie się do ataku osobom bez żadnej wiedzy technicznej. Podobny atak miał miejsce rok wcześniej w Estonii, gdzie przestały działać m.in. oficjalne strony rządowe, serwisy stacji telewizyjnych i agencji prasowych, a także strona policji.

Gruzini broniąc się przed atakami, przenieśli zaatakowane strony na amerykańskie serwery, gdzie te były już bezpieczne. Dzięki temu Gruzini mogli umieszczać oficjalne informacje o sytuacji w kraju. I choć wojna ta trwała jedynie 9 dni, prawdziwy koniec cyberwojny był daleki.

Na początku tego roku Gruzini zidentyfikowali trojana o nazwie Georbot, który działał w dość nietypowy sposób. Atakował komputery urzędników oraz osób współpracujących z Zachodem, a umieszczony był pod linkiem do artykułów o współpracy Gruzji z NATO. Wirus zdążył zaatakować kilkaset komputerów znajdujących

się w ministerstwie, parlamencie i organizacjach pozarządowych. Jego działanie polegało na szpiegowaniu zainfekowanego komputera, gdzie poszukiwał treści związanych z polityką i obronnością kraju. Następnie wirus przekazywał wyszukane treści na wskazany serwer.

Po wykryciu szkodliwego wirusa Gruzini wzięli odwet tworząc zmodyfikowaną wersję Georbota. Postanowili podstępnie podejść wroga i na jednym z zainfekowanych komputerów podłożono archiwum z dokumentem „Porozumienie Rosja-NATO", do którego CERT dołączył zmodyfikowany wirus. Dzięki temu przeszukano komputery włamywacza oraz przejęto kontrolę nad serwerem. I choć podstęp został szybko wykryty, Gruzinom udało się ustalić, że za wrogimi działaniami stoją Rosjanie. Serwer, na który trafiały wykradzione informacje z Gruzji znajdował się pod adresem sąsiadującym z Federalną Służbą Bezpieczeństwa Federacji Rosyjskiej.

Jednak to nie koniec ataków internetowych. Na początku tego miesiąca grupa GhostShell rozpoczęła operację o nazwie Czarna Gwiazda, wymierzoną przeciwko Rosji. Celem akcji jest wykradanie dokumentów pochodzących z różnych instytucji, od polityków oraz służb bezpieczeństwa, a następnie publikowanie ich w sieci. Inicjatorzy tek akcji chcą w ten sposób wyrwać się z tyranii rosyjskich władz, które izolują obywateli od świata.

Choć od pojawienia się informacji na temat tego ataku minęło już trochę czasu, żadne rosyjskie dokumenty do tej pory nie pojawiły się na stronie grupy GhostShell. Stąd można wyciągnąć wniosek, że prawdziwej cyberwojny z Rosją nikt nie chce ryzykować.

Autor: Victor Orwellsky
Na podstawie: www.rferl.org, georgiaonline.ge, www.eurasianet.org
Źródło: Kod Władzy