Cyberszpiedzy w mundurach

11 czerwca 2014

Zachodnim ekspertom ds. bezpieczeństwa udało się zidentyfikować drugą chińską jednostkę wojskową odpowiedzialną za przeprowadzanie cyberataków na europejskie i amerykańskie firmy z branży lotniczej, kosmicznej i telekomunikacyjnej. Już wcześniej powiązano grupę APT1 z Jednostką 61398.

Zdaniem pracowników kalifornijskiej firmy CrowdStrike, działająca od lat grupa „Putter Panda" to część Jednostki 61486 chińskiej armii. Identyfikacji dokonano na podstawie licznych postów, fotografii i rejestru domen dokonanych przez jednego z członków grupy. Człowiek ten, korzystający z nazwiska Chen Ping posiada adresy e-mail i aliasy powiązane z licznymi domenami, na których przechowywane jest szkodliwe oprogramowanie i narzędzia hakerskie. Z wpisów na blogach i witrynach internetowych można dowiedzieć się, że Chen mieszka w Szanghaju i interesuje się bezpieczeństwem IT. Na jednym ze zdjęć widać go w gronie przyjaciół, a w tle widzimy leżące dwie czapki oficerów chińskiej armii. Inne zdjęcie, podpisane „biuro", przedstawia wielkie anteny satelitarne w kompleksie budynków. Wiadomo, że anteny te znajdują się na terenie jednego z budynków w Szanghaju, w którym siedzibę ma jednostka wywiadu elektronicznego. Jakby jeszcze tego było mało, podczas rejestracji jednej z domen Chen podał adres wspomnianego budynku.

„Gdy przyjrzymy się postępowaniu niektórych ludzi zaangażowanych w zaawansowane operacje cyberszpiegowskie, to widzimy, że mogliby być nieco bardziej rozsądni" – mówi George Kurtz, dyrektor firmy CrowdStrike.

Pomimo jednak nierozwagi Chena, sama Jednostka 61486 to trudny przeciwnik. „Mają spory zestaw narzędzi, które sami zbudowali i dość duże możliwości szpiegowskie" – przyznaje Adam Meyers z CrowdStrike.

Autor: Mariusz Błoński
Na podstawie: ComputerWorld
Źródło: Kopalnia Wiedzy