Kolejna grupa hakerów powiązana z chińską armią

27 września 2015

Specjalizujące się w kwestiach bezpieczeństwa firmy ThreatConnect i Defense Group Inc. (DGI) powiązały grupę hakerów Naikon z chińską armią. Zdaniem ekspertów Naikon Advanced Persistent Threat to część Jednostki 78020, która dokonała w przeszłości wielu ataków. Jednostka działa od niemal 5 lat i atakuje głównie firmy w USA posługując się przy tym phishingiem, szkodliwym kodem i pocztą elektroniczną.

Naikon została po raz pierwszy zidentyfikowana w kwietniu 2012 roku przez ShadowServer. To grupa wolontariuszy składająca się z ekspertów ds. bezpieczeństwa. Zajmują się oni zbieraniem informacji o szkodliwym kodzie, botnetach, defraudacjach. Dzięki analizie własnych danych oraz informacji dostarczonych przez hakera Hardcore Charlie, jednego z Anonimowych, który – jak twierdzi – włamał się do chińskich sieci wojskowych – specjaliści z ShadowServer zauważyli istnienie nieznanej wcześniej grupy hakerskiej. Rok później firma TrendMicro opublikowała analizę szkodliwego kodu Rarstone autorstwa Naikon.

Teraz eksperci uważają, że Naikon to część Jednostki 78020, która zajmuje się prowadzeniem cyberataków. Jednostka specjalizuje się w technice phishingu oraz inżynierii społecznej. Precyzyjnie namierza interesujące ją osoby i próbuje w ten sposób dostać się do sieci firm, w których osoby te pracują. Przed atakiem zbierane są takie dane jak imię i nazwisko, adres, data urodzenia, zainteresowania, narodowość, płeć, połączenia społecznościowe czy wcześniej używane e-maile.

ThreatConnect i DGI informują, że udało im się powiązać Naikon z chińską armią dzięki szczegółowej analizie zdobytych

informacji oraz analizie lingwistycznej, podczas której skupili się na oficerze Chińskiej Armii Ludowo-Wyzwoleńczej nazwiskiem Ge Xing.

To już kolejna grupa hakerska, którą zidentyfikowano. Wcześniej pisaliśmy o podobnych analizach łączących hakerów z Jednostkami 61398 oraz 61486.

Autorstwo: Mariusz Błoński
Na podstawie: Enterprise-Security-Today.com
Źródło: KopalniaWiedzy.pl