Cyberdefence 24

aut. Szymon Palczewski 12.12.2018

CYBERATAKI POPRZEDZIŁY KRYZYS NA MORZU AZOWSKIM?

Specjaliści ds. cyberbezpieczeństwa twierdzą, iż wykryli rosyjskie cyberataki wymierzone w ukraińskie wojsko oraz rząd. Incydenty miały miejsce zarówno przed, jak i w trakcie operacji na Morzu Azowskim.

Powiązani z Moskwą hakerzy rozpoczęli skoordynowane działania wymierzone w Kijów jeszcze przed bezpośrednim atakiem rosyjskiej marynarki na ukraińskie statki. Według Stealthcare, grupy wywiadowczej ds. zagrożenia cybernetycznego, cyberataki miały na celu przede wszystkim kradzież informacji istotnych dla zaplanowania całej operacji. Jeśli tezy postawione przez specjalistów są prawdziwe, to znaczy, że całkowitą odpowiedzialność za zapoczątkowanie kryzysu ponosi Rosja.

Moskwa posiada długą historię prowadzenia operacji ofensywnych w cyberprzestrzeni. Mowa tutaj m.in. o działaniach prowadzonych w 2008 roku w Gruzji czy incydentach wymierzonych w Ukrainę, których skutkiem był brak zasilania podczas Świąt Bożego Narodzenia w 2015 roku.

W październiku specjaliści Stealthcare zauważyli, że rosyjski grupa znana jako Carbanak rozwija nową kampanię phishingową, wykorzystującą spreparowane e-maile. Celem cyberprzestępców było zachęcenie użytkowników do kliknięcia w podane linki oraz pobranie złośliwego oprogramowania. Hakerzy ukierunkowali swoje działa przede wszystkim na ukraińskie agencje rządowe.

W złośliwych wiadomościach zamieszczony był plik PDF zawierający odnośniki, które po uruchomieniu umożliwiały cyberprzestępcom kradzież danych oraz kontrolę nad kluczowymi funkcjami komputera. Specjaliści nie mogą na razie wskazać na konkretne jednostki, jakie były celem cyberataku ze względu na wrażliwość całego problemu. Powiedzieli jedynie, iż hakerzy mogli w ten sposób uzyskać dostęp do informacji o ukraińskiej polityki zagranicznej i morskiej, czyli danych, które mogły być niezwykle istotne w trakcie trwania kryzysu. W odniesieniu do całej sprawy Jeremy Samide, przedstawiciel Stealthcare, podkreślił: „Nie ma wątpliwości, że był to wysiłek prowadzonych przez Kreml, którego celem było przygotowanie kryzysu w Cieśninie Kerczeńskiej”.

Druga grupa hakerów powiązana z Moskwą – Gamaredon – uderzyła w ukraińskie agencje rządowe za pomocą złośliwego oprogramowania Pterodo, dostosowanym do systemu Windows. Incydent miał miejsce kilka dni przed 20 listopada, kiedy po raz pierwszy specjaliści Stealthcare poinformowali o wykryciu cyberataków prowadzonych przez Kreml.

26 listopada Rosja przejęła ukraińskie statki i uwięziła ukraińskich marynarzy, a eksperci ds. cyberbezpieczeństwa wskazali na drugi, skoordynowany cyberatak grupy Carbanak. Hakerzy skierowali swoje działania na podmioty wojskowe oraz organy władzy państwowej. Cyberprzestępcy ponownie wykorzystali metody phishingowe w celu kradzieży danych i treści wiadomości e-mail.

Rosyjskie ofensywne cyberoperacje stanowią coraz większe wyzwanie dla państw zachodnich, w tym Stanów Zjednoczonych. Mark Warner, senator Partii Demokratycznej, zauważył, że „kraje takie jak

Rosja coraz częściej łączą cyberataki z tradycyjnymi operacjami informacyjnymi”. Prezentując swoje stanowisko w Center for New American Security w Waszyngtonie dodał – „cyberwojna wykorzystuje największe nasze atuty – naszą otwartość i swobodny przepływ informacji”.