ROSYJSCY HAKERZY NAMIERZYLI UKRAIŃSKĄ ARTYLERIĘ

Rosyjskie złośliwe oprogramowanie pozwoliło na lokalizowanie pozycji ukraińskiej artylerii – podaje Crowd Strike w swoim raporcie. Jego autorem była grupa Fancy Bear powiązana z GRU i odpowiedzialna za ataki na Komitet Partii Demokratycznej.

Ukraińscy żołnierze obsługujący haubice D-30 korzystali z aplikacji opracowanej przez wojsko, która ograniczała proces celowania do zaledwie 15 sekund. Program został jednak zarażony złośliwym oprogramowaniem X-Agent stworzonym przez rosyjskich hakerów z grupy Fancy Bear – podaje raport Crowd Strike.

Na początku 2013 roku jeden z artylerzystów opracował dla siebie oraz swoich kolegów z oddziału aplikację przeznaczoną na Androida. Oprogramowanie nosiło nazwę Попр-Д30.apk i było dostępne tylko dla wybranych osób. Nie pojawiało się na witrynie Google Play, zaś było dystrybuowane za pomocą portalu vKontakte oraz przez stronę autora. Proces aktywacji odbywał się po kontakcie z deweloperem, który przekazywał zainteresowanemu jednorazowy kod do ściągnięcia aplikacji.

X-Agent opracowany przez Fancy Bear był początkowo złośliwym oprogramowaniem przeznaczonym na telefony firmy Apple. Dopiero z czasem został zmieniony, co pozwoliło na instalacje w systemie Android. Według ustaleń Crowd Strike pierwsza wersja Попр-Д30.apk, zarażona X-Agentem, pozwalającym na śledzenie telefonów komórkowych, pojawiła się pod koniec 2014 roku.

Czytaj też: Rasputin zhakował amerykańskie wybory

Rosjanie musieli przechwycić dostęp do aplikacji poprzez kontrolowany przez Kreml portal mediów społecznościowych vKontakte. Autorzy raportu nie dotarli do informacji, w jaki sposób aplikacja została spopularyzowana przez rosyjską stronę konfliktu. Zauważają jednak, że Ukraina odniosła największe straty właśnie w oddziałach posiadających haubice D-30 i korzystających z aplikacji skracającej czas namierzania.

Według danych dostępnych publicznie mowa nawet o stratach sięgających 50 proc. wszystkich dział artyleryjskich oraz 80 proc. w przypadku haubicy D-30 na przestrzeni ostatnich dwóch lat walki. Sam złośliwy kod, X-Agent, nie pozwalał na określenie dokładnej lokalizacji. Jednak miał dawać na tyle dobre rozeznanie, że Rosjanie mogli wysłać w konkretny rejon jeden ze swoich dronów w celu potwierdzenia pozycji ukraińskich wojsk. Oprócz lokalizacji wirus mógł przekazywać Rosjanom treść wiadomości SMS, spis połączeń i dane internetowe. Jak podkreślają autorzy raportu, dane zebrane podczas tych operacji mogą zostać wykorzystane przez Rosjan w przyszłości.