Cyberdefence 24

aut. Szymon Palczewski 22.03.2019

ROSYJSCY HAKERZY W GOTOWOŚCI. EUROWYBORY ZAGROŻONE?

Rosyjscy cyberprzestępcy rozpoczęli nową kampanię hakerską, której celem są europejskie instytucje rządowe. Jak informuje firma FireEye, główną metodą działania hakerów jest spear phishing.

Specjaliści FireEye zaobserwowali aktywność dwóch grup hakerskich sponsorowanych przez państwo (APT28 i Sandworm). Cyberprzestępcy wykorzystywali metodę spear phishingu w celu uzyskania poufnych informacji.

Adresatem fikcyjnych maili były europejskie instytucje rządowe. W treści wiadomości znajdował się link do strony internetowej. Całość wyglądała bardzo autentycznie, co skłaniało ofiary do postępowania zgodnie z instrukcjami wskazanymi w mailu. W wyniku podstępu hakerzy nakłaniali personel instytucji do zmiany haseł za pomocą podanej witryny. W ten sposób cyberprzestępcy uzyskiwali dane niezbędne do logowania do określonych systemów.

Według wielu specjalistów APT28, znana również pod nazwą Fancy Bear, jest grupą hakerską silnie powiązaną z rosyjską agencją wywiadu wojskowego (GRU). Uznaje się ją za złośliwego aktora, który przeprowadził wiele agresywnych kampanii hakerskich.

Odnosząc się do Sandworm specjaliści podkreślają, że jest to grupa, która również ściśle współpracujące z Rosją. Wielu uważa, iż jest ona odpowiedzialna za ransomware NotPetya wymierzony w ukraińskie instytucje.

Obecna kampania hakerska wygląda na skoordynowaną akcję APT28 i Sandworm. Jednak użyte narzędzia podczas ataku różniły się od siebie. Jak informują specjaliści FireEye, firma zauważyła „znaczny wzrost" aktywności obu grup już w połowie 2018 roku, a rosyjska kampania cyberszpiegostwa prowadzona jest nieustannie.

„Hakerzy mogą próbować uzyskać dostęp do sieci w celu zebrania informacji, które pozwolą Rosji na podejmowanie bardziej świadomych decyzji politycznych lub może to być przygotowanie do spowodowania wycieku danych, który byłyby szkodliwy dla konkretnej partii politycznej lub kandydata w kontekście wyborów europejskich" – tłumaczy w specjalnym oświadczeniu Benjamin Read, specjalista FireEye.

Badania i analizy FireEye wywołują obawy o możliwość wpływu Rosji na nadchodzące wybory do Parlamentu Europejskiego. Napięcie wzrasta, ponieważ Moskwa posiada zdolności oraz instrumenty, które sprawnie użyte mogą mieć bezpośredni wpływ na wynik wyborów.

„Związek między tą działalnością (rosyjską kampanią hakerską) a wyborami europejskimi nie został jeszcze potwierdzony, ale płaszczyzna dla ewentualnych ataków jest szeroka" – wskazuje Benjamin Read.

Ostrzeżenie opublikowane przez FireEye pokrywa się z podobnym alertem wydanym przez Microsoft. W zeszłym miesiącu gigant technologiczny poinformował, że hakerzy powiązani z grupą APT28 przeprowadzili kampanie phishingowe wymierzone w think-tanki i organizacje non-profit znajdujące się w Europie.