ROSYJSCY HAKERZY ZNOWU AKTYWNI W WASZYNGTONIE

Rosyjscy hakerzy zaatakowali ambasadę jednego z państw Unii Europejskiej w Waszyngtonie - twierdzą eksperci z firmy ESET zajmującej się cyberbezpieczeństwem.

Grupa hakerska znana również jako Cozy Bear lub The Dukes w swoich działaniach wykorzystuje trzy nowe rodziny złośliwego oprogramowania - PolyglotDuke, RegDuke i FatDuke. Była ona związana z atakami na Narodowy Komitet Partii Demokratycznej USA.

Firma ESET zwróciła uwagę, że rosyjscy cyberprzestępcy w ostatnim czasie pozornie wygasili swoją działalność, jednakże w istocie grupa hakerska wciąż atakuje cele zlokalizowane w państwach członkowskich Unii Europejskiej. Według ekspertów jedne z pierwszych śladów w kampanii, do której należy zaliczyć bieżące cyberoperacje APT29, prowadzą do wpisu na forum Reddit z lipca 2014 roku, który pozwolił specjalistom z dużą pewnością powiązać obserwowaną aktywność hakerską ze sprawcami ataku na Narodowy Komitet Partii Demokratycznej USA (DNC).

Serwis umożliwiający wymianę zdań na forach dyskusyjnych Reddit oraz platforma społecznościowa Twitter to narzędzia, które działający na zlecenie Kremla cyberprzestępcy wykorzystali m.in. do użycia technik steganograficznych w materiałach graficznych. Steganografia to metoda, którą hakerzy mogą wykorzystać do ukrycia złośliwego oprogramowania np. w metadanych pliku graficznego, który z perspektywy użytkownika forum nie budzi żadnych podejrzeń, gdyż jego wygląd pozostaje niezmieniony.

ESET nie ujawnił, które kraje UE zostały zaatakowane przez hakerów, wskazano jednak na trzy państwa oraz placówkę dyplomatyczną jednego z nich zlokalizowaną w Waszyngtonie.

Hakerzy z grupy Cozy Bear zhakowali systemy DNC latem 2015 roku. W kwietniu 2016 roku dokonała tego również inna grupa rosyjskich cyberprzestępców znana jako Fancy Bear. Oba ugrupowania zajmują się hakowaniem w celach szpiegowskich. Celem ich ataku na DNC było przede wszystkim zdobycie danych do logowania w systemie wykorzystywanym przez amerykańską Partię Demokratyczną.