

## ROSJANIE TESTUJĄ NOWĄ CYBERBROŃ NA UKRAINIE

---

**Rosja wykorzystuje nowego wirusa komputerowego do atakowania ukraińskiej infrastruktury krytycznej - poinformował w środę przedstawiciel Służby Bezpieczeństwa Ukrainy (SBU) Ołeksandr Tkaczuk. To kolejna odsłona rosyjskich działań w cyberprzestrzeni prowadzonych przeciwko Ukrainie.**

Nowe wirusy kryjące się pod nazwą "telebot" nie przypominają zwykłego złośliwego oprogramowania, które służy m.in. do wykradania danych osobowych. Zostały zaprojektowane do działań przeciw konkretnym instytucjom - mówił Tkaczuk podczas konferencji prasowej.

Tłumaczył, że ataki zorganizowały rosyjskie siły bezpieczeństwa, współpracując z prywatnymi firmami informatycznymi i hakerami. Wiele wskazuje, że stoją za nimi te same osoby, które wcześniej stworzyły złośliwe oprogramowanie "BlackEnergy" - dodał przedstawiciel ukraińskich sił bezpieczeństwa.

Kijów wielokrotnie oskarżał Rosję o prowadzenie wojny cybernetycznej na Ukrainie. Zarzuty te Moskwa odpiera. "Otrzymaliśmy informacje, że w ataki zaangażowani są nie tylko członkowie rosyjskich służb specjalnych, ale także prywatne firmy z branży IT oraz przestępcze grupy hakerów działające z terytorium Federacji Rosyjskiej" - mówił Tkaczuk. Nie ujawnił, kiedy doszło do tych wydarzeń.

Jak tłumaczył przedstawiciel SBU, kod wirusa został zaprojektowany tak, aby atakować procesy przemysłowe infekując poszczególne części infrastruktury krytycznej. Dla przykładu podał, że w oprogramowaniu znalazły się moduły, które niszczyły konkretne urządzenia sieci energetycznych.

Ukraina alarmuje, że staje w obliczu rosnącej presji cybernetycznej ze strony Rosji. Tylko w listopadzie i grudniu ub. roku odnotowano 6,5 tys. przypadków ataków hakerskich. Władze tego kraju oskarżają cyberprzestępców o sparaliżowanie w grudniu części sieci energetycznej Kijowa, a także o ataki na komputery resortów obrony, finansów a także skarbu państwa.

"Rosyjscy hakerzy i infoboty stali się ważnym narzędziem agresji przeciwko naszemu państwu. (...) Potwierdzili to nasi koledzy z NATO i UE, którzy odnotowali ostatnio rosnącą liczbę ataków na infrastrukturę krytyczną państw Sojuszu i Wspólnoty, prowadzonych przez Rosję lub z terytorium Federacji Rosyjskiej" - dodał Tkaczuk.

Rosja jest podejrzewana o ataki hakerskie m.in. na francuską telewizję TV5Monde, niemiecki parlament i w Bułgarii. Moskwa jest też posądzana o działania podczas ostatnich wyborów prezydenckich w Stanach Zjednoczonych.

O prowadzeniu przez Rosję ciągłej kampanii ataków cybernetycznych wymierzonych w infrastrukturę

krytyczną Zachodu ostrzegł na początku lutego minister obrony Wielkiej Brytanii Michael Fallon. Jego zdaniem te działania mają podważyć podstawy demokracji i osłabić NATO.

W środę rząd Ukrainy wprowadził stan wyjątkowy w sektorze energetycznym. Przyczyną jest poważny deficyt węgla odmiany antracyt, który używany jest w elektrociepłowniach i zakładach metalurgicznych. Minister energetyki i przemysłu węglowego Ihor Nasalyk poinformował, że Ukraińcy mogą liczyć się z przerwami w dostawach prądu. Może to wynikać nie tylko z problemów związanych z dostawami węgla, ale być również efektem cyberataku. Rosjanie doskonale znają infrastrukturę krytyczną Ukrainy i już wcześniej przeprowadzali udane ataki przeciwko elektrowniom. Dlatego niewykluczone, że w przyszłości taka sytuacja może się powtórzyć.

Jak widać Ukraina jest obecnie obszarem testowym dla nowych rodzajów uzbrojenia. Dotyczy to również walki w cyberprzestrzeni. Dlatego sytuację na Ukrainie należy monitorować i wyciągać wnioski, ponieważ wszystkie rodzaje uzbrojenia, które zostaną użyte przeciwko Ukraińcom, może być również wykorzystane przeciwko NATO.

AK/PAP