aut. Szymon Palczewski 27.05.2020

WIELOLETNIA PENETRACJA NIEMIECKICH SIECI PRZEZ ROSJAN. PRZYGOTOWANIA DO CYBERUDERZENIA?

Rosyjscy hakerzy od lat penetrują sieci i systemy niemieckich operatorów infrastruktury krytycznej – alarmują krajowe służby bezpieczeństwa. Głównym celem cyberprzestępców jest uzyskanie dostępu do konkretnych sieci i zbieranie informacji. Jakie zamiary ma Kreml wobec Berlina?

Specjaliści ds. cyberbezpieczeństwa odkryli na początku bieżącego roku dowody „długotrwałych kampanii hakerskich" wymierzonych w niemieckie firmy – donosi serwis CyberScoop, powołując się na państwowe materiały, do których uzyskał dostęp. Specjalne ostrzeżenie zostało rozesłane do operatorów infrastruktury krytycznej przez niemieckie służby bezpieczeństwa i wywiadu.

Grupa hakerska znana jako Berserk Bear została przez specjalistów powiązana z rosyjską FSB. Obecnie jej cyberprzestępcy prowadzą ukierunkowane działania, których celem jest łańcuch dostaw, aby w ten sposób uzyskać dostęp do systemów informatycznych niemieckich firm.

„Celem hakerów jest wykorzystanie publicznie dostępnego, ale także specjalnie opracowanego złośliwego oprogramowania, aby trwale zakotwiczyć się w sieci IT… ukraść informacje, a nawet uzyskać dostęp do konkretnych systemów" – przytacza stanowisko niemieckich służb CyberScoop.

Grupa Berserk Bear jest najbardziej znana z wieloletniej kampanii zbierania danych o amerykańskich firmach energetycznych. Wówczas za złośliwe działania administracja Donalda Trumpa publicznie obwiniła Rosję. To jeden z niewielu zespołów hakerskich, które Moskwa może wykorzystać do zaawansowanego cyberszpiegostwa.

Hakerzy Berserk Bear dbają o to, aby pozostać w ukryciu. Prowadzili operacje nie tylko w Stanach Zjednoczonych, ale także w Europie, gdzie ich celem byli operatorzy infrastruktury krytycznej. Co więcej, w 2018 roku grupa przeprowadziła szeroko zakrojony ogólnoświatowy „rekonesans" w wielu sektorach, w tym branży energetycznej oraz przemysłowej.

„W ciągu ostatnich lat hakerzy byli agresywni i atakowali liczne obiekty" – podkreślił na łamach CyberScoop Robert M. Lee, specjalista firmy Dragos. – „Do tej pory nie pokazali jednak ani możliwości ani zamiaru zakłócania działalności operatorów (infrastruktury krytycznej - przyp. red.). Biorąc jednak pod uwagę fakt, że koncentrują się na przemysłowych systemach kontroli, nadal ich śledzimy i informujemy o nich społeczność".