

ARESztOWANIA HAKERÓW W ROSJI. "PRZYPAD EK, CZY CZYSTKA"?

Aresztowanie trzech członków grupy hakerskiej pracującej dla FSB nie może być przypadkiem. Nie jest jednak jasne, czy działali oni na rzecz obcych wywiadów, o co są oskarżani, czy może są ofiarami wewnętrznych walk w rosyjskich służbach.

W ostatnich dniach, rosyjskie media poinformowały o aresztowaniu dwóch oficerów Centrum Bezpieczeństwa Informatycznego (CIB) Federalnej Służby Bezpieczeństwa Rosji. Jednym z nich jest Siergiej Michajłow – wiceszef CIB i główna osoba odpowiedzialna za politykę cyberbezpieczeństwa, a drugim jego zastępca Dmitrij Dokuczew. Przed dołączeniem do FSB, Dokuczew miał być znanym rosyjskim hakerem. Kiedy został złapany rosyjskie służby postawiły mu ultimatum, współpraca miała być sposobem na uniknięcie więzienia. Wcześniej szef CIB Andriej Gersimow został zwolniony na początku stycznia. Oficjalnym powodem była współpraca z Kaspersky w ściganiu cyberprzestępców. To poważne zmiany w jednej z głównych rosyjskich jednostek odpowiedzialnych za cyberbezpieczeństwo, a w szczególności za działania ofensywne.

Do aresztu trafił również Rusłan Stojanow, menadżer firmy Kaspersky Lab. Kierował on oddziałem ds. badania cyberprzestępstw, współpracując z FSB i Ministerstwem Spraw Wewnętrznych Rosji w analizowaniu przestępstw informatycznych. Bliskie związki Kaspersky Lab z rosyjskimi służbami nie powinny nikogo dziwić, w końcu założyciel firmy Jewgienij Kaspeski zdobył swoje wykształcenie w ośrodku kryptograficznym prowadzonym przez KGB. Do dziś utrzymuje bliskie kontakty z wieloma oficerami wywiadu. Jest m.in. dobrym znajomym Nikołaja Patruszewa - jednego z najbliższych współpracowników Władimira Putina.

Czytaj też: [Menedżer Kaspersky Lab i oficer FSB aresztowani w Rosji](#)

Jak pisze "Nowaja Gazieta", aresztowano jeszcze jednego pracownika FSB, który miał być kolegą Michajłowa. Jego tożsamość pozostaje jednak nieznana. Wszystkich oskarżono o zdradę i przekazywanie informacji CIA, które pozwoliły na stworzenie raportów o rosyjskich atakach hakerskich na systemy wyborcze. Zakres szczegółów zawartych w dokumentach może wskazywać, że powstały one przy wykorzystaniu źródeł osobowych. Nie wskazano też, czy proces wymiany informacji miał odbywać się bezpośrednio czy przez pośredników. Zidentyfikowano również 8 innych osób, które mogą być zamieszane w sprawę.

Michajłow miał przekazywać informacje amerykańskiemu wywiadowi o tzw. King Servers, czyli serwerach hostujących, których właścicielem jest obywatel Rosji Władimir Fomenko. Były one wykorzystywane do ataków na wyborcze systemy komputerowe w Arizonie i Illinois w zeszłym roku. Fomenko oczywiście zaprzeczył tym doniesieniom. Nowaja Gazieta podaje, że rosyjski przedsiębiorca oferował również swoje usługi Pawłowi Wróblewskiemu, który był właścicielem firmy ChronoPay zajmującej się elektronicznymi płatnościami. Został skazany w 2013 roku za serie cyberataków na rosyjskie przedsiębiorstwa, w dużej mierze dzięki staraniom Michajłowa i Stojanowa.

Stojanow został z kolei aresztowany za otrzymywanie pieniędzy od zagranicznych podmiotów. Miał on być łącznikiem pomiędzy Michajłowem a nieznanym zagranicznym przedsiębiorstwem. Pracując dla jednostki ds. walki z cyberprzestępczością w Ministerstwie Spraw Wewnętrznych Stojanow był odpowiedzialny za prawie każde aresztowanie cyberprzestępców w Rosji. W Rosji duża część cyberprzestępców bardzo blisko współpracuje z FSB i dzięki temu nie muszą oni obawiać się aresztowania. Do więzienia trafiają tylko ci, którzy odmówili pomocy rosyjskim służbom lub narazili się władzom.

Bardzo interesującą hipotezę dotyczącą tego wydarzenia zaproponował Brian Krebs, autor książki o rosyjskich cyberprzestępcach. Jego zdaniem za aresztowaniem Stojanowa i Michajłowa stoi wspomniany wyżej Wróblewski, który korzystając z osłabienia pozycji Michajłowa w FSB na skutek walk wewnętrznych dokonał zemsty. Hipoteza ta wydaje się być najbardziej prawdopodobna. Wielokrotnie rosyjscy oficerowie wywiadu ginęli lub byli aresztowani, właśnie na skutek walk wewnętrznych.

Czytaj też: [FSB aresztowała hakera, który opublikował korespondencję Putina](#)

Andriej Sołdatow, badacz rosyjskich służb specjalnych uważa, że cała ta sprawa jest bez precedensu i niszczy ona system relacji komercyjnych firm z agencjami wywiadu, który działał w Rosji od ponad 20 lat. Często administracja rządowa korzystała z rad firmy Kaspersky. Cała ta sprawa wpłynie negatywnie na współpracę służby wywiadowczych Federacji Rosyjskiej z komercyjnym przedsiębiorstwem oraz negatywnie odbije się na reputacji firmy za granicą.

Pojawią się również spekulacje, że hakerzy byli związani z atakami na Stany Zjednoczone podczas wyborów i ich aresztowanie ma być gestem dobrej woli wobec nowej administracji w Białym Domu. Teoria ta wydaje się jednak bardzo mało prawdopodobna, biorąc pod uwagę, że Donald Trump nie przywiązuje do tych włamań większej uwagi. Niektórzy sugerują, że aresztowane osoby należą do rosyjskiej sekcji globalnego ruchu Anonymous znanej jako „Shaltai Boltai” co również wydaje się jednak bardzo mało prawdopodobne. Chociażby ze względu na źródło tej operacji – kremlowską telewizję Tsargrad TV, która słynie z publikowania bardzo mało wiarygodnych materiałów.

Jeżeli zarzuty wobec Michajłowa się potwierdzą będzie to jeden z najwyższych rangą rosyjskich dowódców skazanych za zdradę.

Czytaj też: [Oficer rosyjskiej FSB podejrzany o zdradę stanu](#)