

"IRAŃSCY" ROSJANIE HAKUJĄ NA BLISKIM WSCHODZIE

W sieci zaczyna robić się tłoczno. Irańska grupa hakerska padła ofiarą rosyjskiej grupy cyberprzestępców działającej pod nazwą Turla, która atakowała liczne cele na Bliskim Wschodzie podszywając się pod Irańczyków.

Celem rosyjskiej grupy znanej jako Turla było przejęcie narzędzi którymi posługują się ich irańscy koledzy działający pod nazwą OilRig w celu podszywania się pod ich działania i szpiegowania celów zlokalizowanych w innych krajach. O fakcie tym poinformowało brytyjskie BBC powołując się na informacje z amerykańskiej i brytyjskiej agencji wywiadowczej. Obie agencje potwierdziły, że Rosjanie pozyskują dane zarówno te które ukradzione zostały przez Irańczyków, jak i korzystając z „irańskiego dostępu” prowadzą własne operacje, próbując w ten sposób ukryć ślady.

Odkrycie zostało dokonane już w 2017 roku, kiedy doszło do ataku rosyjskiej grupy na instytucje akademickie w Wielkiej Brytanii. Brytyjskie National Cyber Security Centre (NCSC) odkryło wtedy, że ataku dokonała rosyjska grupa wykorzystując do tego narzędzie irańskiej OilRig.

Łącznie wykryto ataki na cele w ponad 35 krajach, głównie z Bliskiego Wschodu. Działania ukierunkowane były na kradzieże tajemnic i dokumentów, ofiarami stały się również instytucje rządowe. Ofiary mylnie sądziły, że padły ofiarą działań irańskiej grupy, jednak wciąż nie jest jasne czy OilRig był świadomy działań rosyjskiej grupy, ani że czy działania zostały wywołane w celu wywołania napięcia między krajami.

Jak przypomina BBC w czerwcu Symantec upublicznił informację, że Turla wcześniej już działała już w podobny sposób. Ujawnienie informacji przez agencje ma na celu podkreślenie, że pomimo prób ukrycia swojej tożsamości, działania grupy są znane „Chcemy wysłać jasny komunikat, że nawet gdy cyberaktorzy próbują ukryć swoją tożsamość, nasze możliwości są do nich dopasowane i możemy je zidentyfikować” – powiedział dla BBC Paul Chichester dyrektor ds. operacji w NCSN.

Grupa Turla w 2016 i 2017 roku podejrzewana była o ataki na czeskie Ministerstwo Spraw Zagranicznych. Również w 2018 roku byli podejrzewani o atak na sieć komputerową niemieckiego MSZ. Turla uważana jest za jedną z najstarszych i najbardziej wyrafinowanych rosyjskich grup hakerskich sponsorowanych przez państwo.