Cyberdefence 24

aut. Szymon Palczewski 02.12.2019

HAKERSKI ARSENAŁ ZLIKWIDOWANY. SUKCES MIĘDZYNARODOWEGO DOCHODZENIA

Strona internetowa, na której cyberprzestępcy sprzedawali narzędzia hakerskie przeznaczone do prowadzenia cyberataków, została zlikwidowana w wyniku międzynarodowej operacji. W działania zaangażowane były między innymi brytyjskie, australijskie oraz unijne służby.

Brytyjska National Crime Agency (NCA) poinformowała, że około 14 500 osób z różnych części świata kupiło specjalistyczne narzędzie szpiegowskie ze strony Imminent Methods. Złośliwy trojan Imminent Monitor Remote Access (IM RAT) był dostępny za jedyne 25 USD – czytamy w oficjalnym komunikacie na stronie NCA.

Zainstalowanie trojana IM RAT na komputerze ofiary umożliwiało hakerom uzyskanie pełnego dostępu do zainfekowanego urządzenia, dzięki czemu cyberprzęstępcy mogli m.in. wyłączyć oprogramowanie antywirusowe, wykraść dane lub hasła, rejestrować poruszanie się użytkownika po klawiaturze czy obserwować ofiary za pomocą wbudowanej kamerki.

Jak wskazuje NCA, międzynarodowa operacja była prowadzona przez Australian Federal Police (AFP) wraz z North West Regional Organised Crime Unit (NWROCU), która odpowiadała za działania na obszarze Wielkiej Brytanii. Jednym z podmiotów koordynujących akcję była National Crime Agency.

W wyniku dochodzenia aresztowano 14 osób w związku ze sprzedażą oraz wykorzystaniem złośliwego oprogramowania. Ostatecznie australijskie służby usunęły witrynę 29 listopada br.

„Współpracując z NWROCU, AFP oraz innymi międzynarodowymi partnerami, mogliśmy przyczynić się do usunięcia strony internetowej, która rozpowszechniała złośliwe oprogramowanie i wspierała działalność hakerską” – stwierdził Phil Larratt, przedstawiciel NCA. „IM RAT był używany przez osoby fizyczne i zorganizowane grupy przestępcze w Wielkiej Brytanii do popełniania szeregu przestępstw, w tym oszustw, kradzieży i szpiegostwa”.

Z kolei jak wskazał Andy Milligan z NWROCU, prowadzona operacja była wymagającym śledztwem o zasięgu międzynarodowym. Ekspert zaznaczył, że działania zaangażowano inne agencje, w tym Europol oraz Eurojust. Dodał, że wszyscy użytkownicy powinni postępować zgodnie z instrukcjami National Cyber Security Center (NCSC) w celu poprawy swojego bezpieczeństwa.

Czytaj też: Europol uderza w serwery ISIS. Cios w propagandę Państwa Islamskiego