aut. Szymon Palczewski 10.05.2021

WYNAJMOWALI INFRASTRUKTURĘ HAKEROM. GROZI IM DO 20 LAT WIĘZIENIA

Obywatele państw z Europy Wschodniej przyznali się do prowadzenia niezgodnej z prawem działalności, polegającej na świadczeniu usług tzw. „kuloodpornego hostingu" na rzecz podmiotów cyberprzestępczych. Oskarżeni pomagali wrogim grupom w prowadzeniu operacji hakerskich poprzez m.in. wynajmowanie adresów IP, serwerów i domen, które były wykorzystywane do rozpowszechniania złośliwego oprogramowania. W ten sposób posłużyli się do powstania strat finansowych sięgających milionów dolarów. Grozi im do 20 lat więzienia.

34-letni Aleksandr Grichishkin i 34-letni Andrei Skwortsow z Rosji, 33-letni Aleksandr Skorodumow z Litwy oraz 30-letni Pawel Stassi z Estonii przyznali się do udziału w spisku, mającym na celu świadczenie usług dla cyberprzestępców z zakresu tzw. „kuloodpornego hostingu" (ang. bulletproof hosting) w latach 2008-2015 – poinformował amerykański Departament Sprawiedliwości. Mężczyźni działali w ramach organizacji Racketeer Influided Corrupt Organisation (RICO).

Zgodnie z dokumentacją sądową oskarżeni byli „założycielami i/lub członkami organizacji" i „wynajmowali cyberprzestępcom adresy IP, serwery oraz domeny, którzy wykorzystywali tę infrastrukturę do rozpowszechniania złośliwego oprogramowania". Wirusy były używane przede wszystkim do uzyskiwania dostępu do urządzeń ofiar, kradzieży danych uwierzytelniających do kont bankowych czy tworzenia botnetów w celu popełniania oszustów.

Jak wskazuje Departament Sprawiedliwości USA, złośliwe oprogramowanie hostowane przez RICO obejmowało takie wirusy takie jak Zeus, SpyEye, Citadel i Blackhole Exploit Kit, które w latach 2009-2015 były wykorzystywane podczas wzmożonych cyberataków na amerykańskie firmy i instytucje finansowe. Doprowadziło to do strat liczonych w milionach dolarów.

Dlaczego usługa świadczona przez obywateli z Europy Wschodniej nazywa się „kuloodpornym hostowaniem"? Wynika to z faktu, że jednym z głównych zadań mężczyzn było udzielenie pomocy ich klientom w uniknięciu wykrycia wrogich działań przez organy ścigania, a przez to możliwości dalszego prowadzenia kampanii cyberprzestrzępczych.

Każdemu z oskarżonych grozi maksymalna kara 20 lat pozbawienia wolności. FBI przeprowadziło dochodzenie w sprawie we współpracy z organami ścigania z Niemiec, Estonii i Wielkiej Brytanii – informuje Departament Sprawiedliwości USA.

Czytaj też: Cyberatak na sieć rurociągów paliwowych w USA. Oskarżenia w kierunku Rosji