aut. Piotr Mieszkowski 27.04.2017

INTERPOL UDERZA W SERWERY CYBERPRZESTĘPCÓW

Interpol przeprowadził dużą operację w Azji. Polegała ona na zidentyfikowaniu setek stron internetowych, które są zagrożone działaniami ze strony grup cyberprzestępczych. Badanie prowadzone przez Interpol doprowadziły do odkrycia około 9 tys. serwerów dowodzenia i kontroli i setek zainfekowanych stron internetowych.

Interpol Global Complex for Innovation (IGCI) przeprowadził we współpracy z partnerami z Indonezji, Malezji, Myanmaru, Filipin, Singapuru, Tajlandii i Wietnamu operacje wymierzoną w cyberprzestępców. Organizacja została wsparta przez firmy sektora prywatnego: Trend Micro, Kaspersky Lab, Cyber Defense Institute, Booz Allen Hamilton, British Telecom, Fortinet i Palo Alto Networks.

Rezultat akcji to odkrycie 270 zainfekowanych stron internetowych, w tym niektórych agencji rządowych, a także identyfikacja kilku podmiotów zajmujących się witrynami phishingowymi. Ponadto znaleziono blisko 9 tys. serwerów C&C ukierunkowanych na rozpowszechnianie ransomware, spamu i przeprowadzanie ataków DDoS.

Badacze twierdzą, że operacja ta jest pierwszym krokiem w likwidacji różnych operacji cyberprzestępczych w tym regionie Azji. Agencje egzekwowania prawa z państw ASEAN nadal badają nabywane, zainfekowane serwery C&C i próbują zidentyfikować stojących za tym cyberprzestępców.

Czytaj też: Cyberszpiedzy atakują niemieckie partie przed wyborami

Śledztwo Interpolu obejmowało wiele grup i operacji związanych z cyberprzestępczością, a niektóre strony internetowe i serwery, które padły ofiarą hakerów były czyszczone lub przenoszone w tryb offline. Działanie Interpolu nie koncentrowało się na likwidacji serwerów C&C, a raczej na identyfikowaniu ich w celu prowadzenia dalszego dochodzenia.

Jak poinformował serwis darkreading.com rzecznik Interpolu, akcja była szeregiem działań podejmowanych przez zaangażowane w to kraje. Zaznaczył jednak, że kraje uczestniczące nadal badają specyfikę i stopień zaawansowania należących do grup hakerskich serwerów dowodzenia i kontroli, ich aktywność oraz czy istnieje możliwość zidentyfikowania cyberprzestępców.