aut. Szymon Palczewski 30.11.2020

NATO PRZETESTOWAŁO (CYBER)ZASADZKI. WRÓG SAM „ODKRYWA KARTY”

NATO przetestowało skuteczność zastosowania honeypots w odniesieniu do operacji wrogich hakerów podczas ostatniej edycji największych wirtualnych ćwiczeń sojuszu „Cyber Coalition 2020”. Tego typu metoda walki z przeciwnikiem jest stosunkowo nowym rozwiązaniem, które w przeszłości zostało użyte między innymi podczas wyborów prezydenckich we Francji. NATO chce udoskonalić swoje zdolności i poznać sposób działania wroga.

Podczas ostatnich ćwiczeń NATO „Cyber Coalition 2020”, które miały miejsce od 16 do 20 listopada br. siły sojuszu koncentrowały się na zastosowaniu honeypots w taki sposób, aby przeciwnik mógł przeprowadzić skuteczny cyberatak na infrastrukturę, która jest w pełni kontrolowaną przez specjalistów. W wydarzeniu wzięło udział 1000 ekspertów ds. cyberbezpieczeństwa z 29 państw członkowskich oraz 4 krajów partnerskich.

Na pierwszy rzut oka wydaje się, że tego typu podejście jest bezsensowne i nie ma nic wspólnego z cyberbezpieczeństwem. W rzeczywistości jednak przeciwnik może złamać zabezpieczenia jedynie wybranych urządzeń lub systemów, które zostały do tego przygotowane (na przykład wyczyszczone z poufnych danych lub celowo zamieszczono na nich fałszywe informacje). W ten sposób wrogi aktor jest przekonany, że jego operacja zakończyła się sukcesem i dalej zaczyna penetrować sieci, do jakich uzyskał dostęp, demaskując przy tym swoje narzędzia oraz metody działania.

O skupieniu się na honeypots w ramach listopadowych ćwiczeń poinformował Alberto Domingo, dyrektor techniczny ds. cyberprzestrzeni NATO, podczas spotkania z dziennikarzami podsumowując wydarzenia. Jak wskazał, symulacje pokazały zalety tego typu „oszustwa”, ponieważ pozwala ono na działanie przeciwko adwersarzowi bez jego wiedzy – przytacza stanowisko przedstawiciela sojuszu serwis Defense One.

Skuteczność potwierdzona w praktyce?

Deborah Frincke, była dyrektor ds. badań w NSA, wskazała podczas swojego przemówienia w ramach National Defense Industry Association w 2017 roku, że honeypots są skutecznym narzędziem ze względu na fakt, że pozwalają uzyskać „wgląd w sposób myślenia przeciwnika”. W ten sposób osoby odpowiedzialne za cyberbezpieczeństwo mogą uzyskać odpowiedź na wiele kluczowych pytań, takich jak: Jak działa przeciwnik? Co zrobi zanim przeprowadzi cyberatak? Jakich narzędzi używa? Jaki jest jego poziom zaawansowania?

Serwis Defense One przypomina, że zastosowanie honeypots w rzeczywistości faktycznie może okazać się skuteczne, co potwierdzają działania przeprowadzone przez francuskich specjalistów. W maju 2017 roku miały miejsce wybory prezydenckie, w których zwyciężył Emmanuel Macron. Wówczas hakerzy rosyjskiego wywiadu GRU próbowali ingerować w kampanię obecnego prezydenta Francji.

Dyrektor ds. kampanii cyfrowych Mounir Mahjoubi wskazał w tamtym okresie na łamach New York Times, że rosyjskie służby wpadły w pułapkę. Francuzi stworzyli fake'owe konta z fałszywą treścią i to na masową skalę, aby znacznie utrudnić działanie i tym samym opóźnić operacje Moskwy.