Cyberdefence 24

aut. Sylwia Gliwa 27.11.2020

TRICKBOT JUŻ PO REANIMACJI

Operatorzy Trickbota reanimują największy botnet świata – twierdzi analiza przeprowadzona przez ekspertów Bitdefender. Wygląda na to, że operacja Microsoftu była jedynie działaniem krótkoterminowym i ukierunkowana była na zabezpieczenie wyborów.

Wygląda na to, że Tricktbot wciąż próbuje się odrodzić. Eksperci z Bitdefender odkryli, że pomimo szumnie ogłoszonej akcji, w której udział brał m.in. Microsoft operatorzy wciąż próbują postawić go „na nogi". „TrickBot mógł doznać poważnego ciosu, ale wydaje się, że jego operatorzy starają się przywrócić go do życia, potencjalnie w jeszcze bardziej odpornej i trudniejszej do zwalczenia niż kiedykolwiek wcześniej formie" – wskazują w swojej analizie.

Przypomnijmy, że na początku października Microsoft wraz z szeregiem innych podmiotów ogłosił przeprowadzenie operacji mającej na celu wyłączenie Trickbota. Pomimo początkowej euforii okazało się, że nie udało się zamknąć botnetu z sukcesem, a jego komponenty w dalszym ciągu funkcjonują, a sam Microsoft przyznał od momentu uruchomienia operacji do 18 października wyłączono 120 ze 128 zidentyfikowanych serwerów rozlokowanych na całym świecie. Jak jednak przewiduje amerykański koncern, liczby te stale będą podlegać modyfikacji wraz z kolejnymi działaniami zarówno grupy jak i cyberprzestępców.

Eksperci Bitdefender w swoim wpisie na blogu porównują przeprowadzoną operację do „strzałów w kolana, ale nie obcinania głów hydrze". „Była to prawdopodobnie taktyka krótkoterminowa, potencjalnie po to, aby upewnić się, że TrickBot nie spowoduje żadnych problemów podczas wyborów" – wskazano w analizie.

Czym jest Trickbot?

Trickbot to sieć serwerów i zainfekowanych urządzeń prowadzonych przez przestępców odpowiedzialnych za szeroki zakres niecnych działań, w tym za dystrybucję oprogramowania ransomware, które może blokować systemy komputerowe. Trickbot jest jednym z największych i najdłużej działających botnetów w sieci.

Pierwsza jego działalność została wykryta pod koniec 2016 roku i pomimo, że tożsamość operatorów nie jest znana – dotychczasowe badania przeprowadzone na przestrzeni tych lat pozwalają wyciągnąć wniosek, że służą one zarówno państwom jak i sieciom przestępczym.

Przewiduje się, że właśnie od 2016 roku Trickbot zainfekował ponad milion urządzeń zlokalizowanych na całym świecie. Był on wykorzystywany m.in. do prowadzenia kampanii spamerskich i phishingowych przy społecznie ważnych tematach jak Black Lives Matter i COVID-19.

Oprócz zagrożenia wyborami Trickbot, jak podkreśla Microsoft, jest wykorzystywany również do docierania do witryn bankowości internetowej oraz kradzieży środków finansowych od ludzi i instytucji. Botnet atakował instytucje finansowe, od globalnych banków i podmiotów obsługujących

płatności po regionalne spółdzielcze kasy pożyczkowe.

Czytaj też: Nieudana misja USCYBERCOM. Trickbot „wraca do żywych”