RAPORT: PRZYBYWA UKIERUNKOWANYCH CYBERATAKÓW

Specjaliści obserwują rosnąca liczbę ukierunkowanych cyberataków mających na celu wyłudzenie pieniędzy. Pretekstem do wyłudzeń może się stać w przyszłości również rozporządzenie o ochronie danych osobowych (RODO) - wynika z wtorkowego raportu Trend Micro.

Zgodnie z raportem "Security Roundup for 2017: The Paradox of Cyberthreats" w ostatnich 12 miesiącach wzrosła liczba ataków z użyciem oprogramowania ransomware, fałszywych biznesowych wiadomości e-mail (ang. Business E-mail Compromise, BEC) oraz wydobywających kryptowaluty, a cyberprzestępcy stale doskonalą swoje techniki. Nowy raport potwierdza wcześniejsze prognozy specjalistów, którzy przewidywali między innymi spadek znaczenia "ataków na oślep" (ang. spray-and-pray) na rzecz strategicznych ataków ukierunkowanych.

Analitycy przewidują, że w 2018 roku do dotychczasowych ataków dołączą próby wyłudzenia okupu od przedsiębiorstw i instytucji chcących uniknąć naruszenia nowych unijnych przepisów o ochronie danych osobowych. Zdaniem specjalistów cyberprzestępcy mogą domagać się od zaatakowanych organizacji okupów o niższej wartości, niż przewidywane przez RODO kary. Może się to przyczyniać to utrzymania dotychczasowych praktyk, tak jak w wypadku wycieku danych 57 mln użytkowników Ubera, który firma starała się zatuszować, płacąc hakerom 100 tys. dolarów. Zdarzenie ujawnił dopiero nowy prezes Dara Khosrowshahi - ponad rok po tym, jak doszło do ataku.

"Raport za rok 2017 pokazuje, że rodzaje zagrożeń zmieniają się w zawrotnym tempie. Cyberprzestępcy wiedzą, że mogą zarabiać na swoim procederze jeszcze więcej, gdyż firmy nie zechcą ryzykować utraty pieniędzy, danych czy reputacji — a takie mogą być konsekwencje strategicznych ataków wymierzonych w najcenniejsze zasoby przedsiębiorstwa" — podał w komunikacie dyrektor działu komunikacji ds. globalnych zagrożeń w firmie Trend Micro, Jon Clay.

Analitycy wskazują również na utrzymujący się wysoki stopień narażenia sprzętów łączących się z internetem na ataki cyberprzestępców. Urządzenia wchodzące w skład internetu rzeczy (IoT) bywają wykorzystywane nie tylko do formowania botnetów, takich jak Mirai, do przeprowadzania ataków typu DDoS, lecz coraz częściej również do generowania (inaczej - kopania) kryptowalut. W ciągu całego ubiegłego roku firma Trend Micro odnotowała ponad 45,6 mln podobnych przypadków.

Założona w Stanach Zjednoczonych firma Trend Micro prowadzi działalność w dziedzinie zabezpieczeń cybernetycznych. Spółka zatrudnia ponad 6 tys. pracowników w przeszło 50 krajach świata, między innymi w Polsce. Światowa siedziba firmy znajduje się w Tokio w Japonii.