FALA ATAKÓW RANSOWMARE NA BRYTYJSKIE SZKOŁY I UNIWERSYTETY

Od sierpnia br. nastąpił gwałtowny wzrost liczby cyberataków wymierzonych w brytyjskie placówki edukacyjne. Hakerzy posługują się oprogramowaniem ransomware, wykorzystując podatności w systemach oraz sieciach instytucji. Większa aktywność cyberprzestępców wiąże się z powrotem uczniów do szkół i studentów na uczelnię.

Specjaliści brytyjskiej National Cyber Security Centre (NCSC) zaobserwowali wzrost liczby cyberataków na podmioty z sektora edukacyjnego, który trwa od sierpnia br. Ich zdaniem jest to związane z powrotem roku szkolnego oraz akademickiego. Ransomware stanowi główną metodę działania hakerów.

NCSC wskazało, że poradziło sobie z kilkoma cyberatakami, lecz część z nich pociągnęła za sobą negatywne konsekwencje, co wynikało ze słabszego poziomu bezpieczeństwa placówek edukacyjnych, będących celem hakerów.

„Od sierpnia 2020 roku NCSC bada zwiększoną liczbę ataków z udziałem oprogramowania ransomware na brytyjskie placówki edukacyjne, w tym szkoły, uczelnie i uniwersytety" – czytamy w oficjalnym alercie wydanym przez specjalistów.

NCSC zaleca, aby organizacje wdrożyły strategię „dogłębnej obrony" na rzecz ochrony przed atakami złośliwego oprogramowania, w tym ransomware. Specjaliści wskazują między innymi na konieczność tworzenia kopii zapasowych danych, a także ich przechowywanie poza siecią w „trybie offline".

„Cyberataki na sektor edukacji, szczególnie w tak trudnym czasie, są całkowicie niedopuszczalne" – podkreślił Paul Chichester, dyrektor operacyjny NCSC. Równocześnie zachęcił wszystkie instytucje kształcące do zwrócenia uwagi na czujność w cyberprzestrzeni i podjęcie odpowiednich kroków, aby zapewnić młodym ludziom możliwość niezakłóconego powrotu do edukacji.

„Jesteśmy zobowiązani do zapewnienia, że brytyjskie środowisko akademickie jest tak bezpieczne, jak to tylko możliwe (…) i nie zawahamy się działać, gdy to zagrożenie ewoluuje" – zadeklarował Paul Chichester.

NCSC przypomina, że ransomware to rodzaj złośliwego oprogramowania, które uniemożliwia użytkownikowi dostęp do systemów lub przechowywanych na urządzeniu danych. Najczęściej dochodzi do ich zaszyfrowania, ale mogą też zostać usunięte lub skradzione. Po skutecznym przeprowadzeniu cyberataku hakerzy zazwyczaj żądają okupu w zamian za odzyskanie dostępu do danego nośnika bądź pliku.

„Ataki ransomware mogą mieć druzgocący wpływ na organizacje, a ofiary potrzebują dużo czasu na przywrócenie sprawnego funkcjonowania systemów" – tłumaczy NCSC. Specjaliści wskazują, że jedną

z popularniejszych metod hakerskich wykrytych w ostatnim czasie przez ekspertów jest wykorzystanie podatności oprogramowania lub całego sprzętu. „Niezabezpieczone urządzenia są często wykorzystywane przez hakerów do instalowania oprogramowania ransomware jako łatwej drogi do sieci docelowej” – czytamy w komunikacie.

Kolejną popularną metodą, jaką wyróżnia NCSC są e-maile phishingowe. Wiadomości tego typu zachęcają użytkowników do otworzenia zainfekowanego pliku lub kliknięcia w złośliwe łącze, przez co dochodzi do zainstalowania oprogramowania ransomware na danym nośniku.

Po uzyskaniu dostępu do sieci hakerzy przeszukują system w celu znalezienia „celu o wysokiej wartości”, często używając innych narzędzi. Dodatkowo podejmują działania na rzecz zatarcia śladów, aby w ten sposób utrudnić późniejsze śledztwo i zbadanie incydentu.

David Corke, przedstawiciel Association of Colleges, zaznaczył, że ostatnie sześć miesięcy pokazało, że uczelnie oraz inne placówki edukacyjne muszą posiadać odpowiednią infrastrukturę cyfrową, aby chronić swoje systemy i zagwarantować ciągłość nauczania niezależnie od okoliczności. „Wymaga to podejścia całej instytucji, a z szerszej perspektywy, musi obejmować wsparcie liderów, nauczycieli i uczniów w rozpoznawaniu zagrożeń, ich łagodzeniu oraz zdecydowanemu działaniu, gdy tylko coś pójdzie nie tak” – podkreślił Corke.

Jak wskazuje NCSC, instytucje, które zostały zainfekowane oprogramowaniem ransomware, zauważyły, że ich zdolność do skutecznego działania i świadczenia usług jest znacznie utrudniona. W zależności od poziomu odporności danej organizacji może minąć kilka tygodni, a w niektórych przypadkach nawet miesięcy, zanim usługi wrócą do normy.

Czytaj też: Pierwsza ofiara śmiertelna ataku ransomware. Zarzut nieumyślnego spowodowania śmierci