Cyberdefence 24

aut. Szymon Palczewski 22.05.2020

RUMUŃSKA POLICJA O KROK PRZED HAKERAMI. GRUPA PLANUJĄCA SPARALIŻOWANIE SZPITALI ROZBITA

Hakerzy planujący przeprowadzenie zorganizowanego cyberataku na szpitale w Rumunii zostali aresztowani przez lokalną policję. W trakcie przeszukania zatrzymanych znaleziono narzędzia hakerskie, w tym popularne trojany zdalnego dostępu. Sparaliżowanie placówek medycznych miało być wyrazem protestu przeciwko wprowadzonym przez rząd restrykcjom związanym z pandemią COVD-19.

Rumuńska policja aresztowała czterech hakerów, w wieku od 20 do 30 lat, którzy byli członkami grupy cyberprzestępczej znanej w środowisku jako PentaGuard. Funkcjonariusze podczas przeszukania domów zatrzymanych znaleźli dowody, jednoznacznie wskazujące na chęć przeprowadzenia ataków ransomware na rumuńskie szpitale – donosi ZDNet.

Rumuńska Dyrekcja ds. Badania Przestępczości Zorganizowanej i Terroryzmu (DIICOT) potwierdziła, że członkowie grupy posiadali złośliwe oprogramowanie, takie jak trojany zdalnego dostępu i oprogramowanie ransomware, które miało być wykorzystane do zakłócenia funkcjonowania lokalnych placówek ochrony zdrowia.

„Uzyskane dotychczas informacje wykazały, że zamierzają w niedalekiej przyszłości rozpocząć złośliwą kampanię, w tym ransomware, wymierzoną w niektóre publiczne instytucje opieki zdrowotnej w Rumunii, głównie szpitale" – czytamy w informacji prasowej DIICOT.

Rumuńskie służby wskazują, że hakerzy zamierzali podszyć się pod urzędników państwowych i rozsyłać złośliwe e-maile do instytucji zdrowia publicznego. „Wabikiem" miał być temat wiadomości dotyczący koronawirusa – informuje CyberScoop.

Planowane cyberataki miały stanowić formę protestu przeciwko wprowadzonym obostrzeniom. „Chcieli się zemścić (przyp. red. hakerzy) na władzach, które wprowadziły stan wyjątkowy" – podaje rumuński dziennik Stirile Pro Tv.

Według firmy zajmującej się cyberbezpieczeństwem KELA, grupa PentaGuard istnieje od 2000 roku. Ich działalność do tej pory była znana z przeprowadzania zmasowanych cyberataków w celu zniszczenia stron rządowych oraz witryn wojskowych – informuje ZDNet.

DIICOT alarmuje, że tego typu kampanie wymierzone w placówki ochrony zdrowia są znacznie groźniejsze, ponieważ mogą mieć bezpośredni wpływ na ludzkie życie. „Poprzez cyberataki istnieje możliwość zablokowania i poważnego zakłócenia funkcjonowania infrastruktury IT szpitali, które odgrywają obecnie decydującą rolę w walce z pandemią COVID-19" – podkreślają specjaliści DIICOT.

Wraz z wybuchem pandemii koronawirusa zaobserwowano wzrost złośliwych kampanii wymierzonych nie tylko w instytucje ochrony zdrowia, ale także placówki badawcze pracujące nad szczepionką oraz lekami zwalczającymi COVID-19.

O problemie poinformował również Interpol, który ostrzegł partnerów przed intensyfikacją działalności hakerów w ostatnim czasie. „Centrum Cyber Fusion wykryło znaczny wzrost liczby prób ataków ransomware na kluczowe organizacje i infrastrukturę zaangażowaną w walkę z wirusem" – czytamy na oficjalnej stronie Interpolu. – „Hakerzy używają oprogramowania ransomware do cyfrowego paraliżowania szpitali i usług medycznych, uniemożliwiając im dostęp do kluczowych systemów i danych".