Cyberdefence 24

aut. Sylwia Gliwa 13.11.2019

OKUP W BITCOINACH I BRAK MOŻLIWOŚCI DOKONYWANIA PŁATNOŚCI. HAKERZY UDERZAJĄ W PRZEDSIĘBIORSTWO NAFTOWE

Meksykańskie przedsiębiorstwo naftowe w tarapatach. Równowartość 5 milionów dolarów w bitcoinach zażądali hakerzy od państwowej firmy naftowej jako okupu za odblokowanie zainfekowanych systemów. Pracownik korporacji mówi o możliwych problemach z dokonywaniem płatności z uwagę na blokadę komputerów.

Włamanie do wewnętrznych systemów firmy Pemex odnotowano w niedzielę. Skutecznie uniemożliwiło ono pracę przedsiębiorstwa i zmusiło do wyłączenia komputerów oraz zamrożenia systemów odpowiedzialnych za płatności – twierdzi Reuters, powołując się na pracowników przedsiębiorstwa. Na komputerach miała pojawić się notatka z żądaniem okupu, która wskazywała na darknetową stronę internetową powiązaną z „DoppelPaymer" (rodzajem oprogramowania ransomware), gdzie widniał 48-godzinny termin płatności 565 bitcoinów (ok. 5 milionów dolarów) oraz adres e-mail do kontaktu.

Reuters skontaktował się z hakerami za pośrednictwem podanego adresu e-mail i otrzymał informacje, że kwota wynika z braku reakcji na zaproponowaną przez cyberprzestępców „cenę promocyjną". Sama spółka odmówiła komentarza odnośnie żądania okupu i przekazała, za pośrednictwem oświadczenia, że atak wpłynął na mniej niż 5% komputerów, a urządzenia do przechowywania i dystrybucji działają normalnie.

Jedno z wewnętrznych źródeł Reutersa potwierdziło, że firma jest celem oprogramowania „Ryuk", będące rodzajem ransomware. Wykorzystany DoppelPaymer jest również stosunkowo nową odmianą ransomware, które zostało wykorzystane także podczas ataku na chilijskie Ministerstwo Rolnictwa i miasto Edcouch w Teksasie.

We wtorek firma ponownie podłączała niezainfekowane komputery do sieci oraz czyściła zainfekowane jednostki. Przeniesiono komunikację pomiędzy pracownikami na platformę WhatsApp z uwagi na brak możliwości wykorzystywania firmowych skrzynek e-mail.