Cyberdefence 24

aut. Szymon Palczewski 10.11.2020

WIELCY IZRAELSKIEGO BIZNESU OFIARAMI RANSOMWARE. KTO STOI ZA CYBERATAKAMI?

Hakerzy uderzyli w duże izraelskie korporacje wykorzystując do tego celu opracowane zupełnie od podstaw oprogramowanie ransomware. Z każdym dniem pojawiają się nowe doniesienia o kolejnych poszkodowanych firmach. Komu zależy na sparaliżowaniu izraelskich podmiotów?

W ciągu ostatnich dni „wyjątkowo dużo liczba" izraelskich firm zgłosiła ataki ransomware –wskazują specjaliści Check Point Research. Pierwsze wrogie działania miały miejsce pod koniec października br. i głównie były przeprowadzane w godzinach nocnych (zwykle po północy), kiedy pracownicy IT wielu firm nie pracują.

Część operacji hakerskich została przeprowadzona przez popularne warianty złośliwego oprogramowania, takie jak REvil czy Ryuk. Jednak kilka dużych korporacji doświadczyło cyberataku z użyciem nieznanej wcześniej odmiany ransomware, nazwanej przez ekspertów „Pay2Key". Specjaliści nie wskazali jednak konkretnych nazw poszkodowanych podmiotów prawdopodobnie dlatego, aby zadbać o ich bezpieczeństwo i ochronę interesów.

> *Analizując działanie Pay2Key, nie byliśmy w stanie połączyć go z żadnym innym istniejącym szczepem ransomware i wydaje się, że jest on tworzony całkowicie od podstaw*
>
> *Fragment raportu „Ransomware Alert: Pay2Key" opracowanego przez Check Point Research.*

Dotychczasowa analiza incydentów wykazała, że podmiot odpowiedzialny za operacje mógł uzyskać dostęp do sieci organizacji będącej celem na długo przed realizacją cyberataków. Wykorzystywał do tego słabo zabezpieczone usługi RDP (Remote Desktop Protocol) w korporacjach.

W ciągu godziny wirus rozprzestrzeniał się w całej sieci ofiary. Po zakończeniu fazy infekcji ofiary otrzymały spersonalizowany list z żądaniem okupu. Jego wysokość w zależności od organizacji wahała się między 7-9 bitcoinów (407 064-523 368 zł.).

Co ciekawe, w komunikacie, który pojawiał się na ekranie ofiary po infekcji, zamieszczono wpis mówiący, że bezpieczeństwo danych zostało naruszone, lecz specjaliści nie znaleźli jak dotąd żadnych dowodów potwierdzających taki stan rzeczy.

Pomimo, że tożsamość podmiotu stojącego za cyberatakami nie jest znana, niespójne angielskie sformułowania w różnych ciągach znaków znajdujących się w kodzie sugerują, że dla hakerów język

angielski nie jest językiem wrodzonym.

> *Ataki były wymierzone w izraelski sektor prywatny, ale patrząc na taktykę, techniki i procedury operacji, obserwujemy potężnego aktora, który nie ma powodów, aby ograniczać się wyłącznie do ograniczonej listy celów w Izraelu*
>
> *Treść raportu Check Point Research.*

Ransomware stanowi jedno z najpoważniejszych wyzwań dla cyberbezpieczeństwa. Zauważył to między innymi Europol, który w specjalnym raporcie poświęconym ryzyku w sieci podkreślił, że „ransomware pozostaje jednym z najbardziej dominujących zagrożeń, zwłaszcza dla organizacji publicznych i prywatnych" w skali świata.

W ostatnim czasie rośnie liczba poważnych cyberataków z udziałem oprogramowania szyfrującego. W tym miejscu można wskazać chociażby na incydenty z udziałem prywatnych firmy: producenta alkoholu „Campari", największego pod względem dochodów producenta zabawek „Mattel" oraz ukraińskiego dostawcy usług IT i twórcy oprogramowania koncern „SoftServe".

Hakerzy jednak skupiają swoją uwagę również na sektorze państwowym, co obrazują cyberataki na przykład na: Trybunał Sprawiedliwości Brazylii, spółkę transportu publicznego z Montrealu, a także Departament Transportu Teksasu.

Ransmoware jest szczególnie groźne, gdy zostaje wymierzone w podmioty ochrony zdrowia. Niestety od momentu wybuchu pandemii koronawirusa hakerzy przeprowadzają coraz większą ilość wrogich działań, których celem są szpitale oraz inne instytucje z branży medycznej. Wynika to z faktu, że ich znaczenie w czasie kryzysu zdrowotnego jest szczególne i nie mogą sobie pozwolić na zakłócenie lub zawieszenie działalności. W związku z tym często ulegają presji cyberprzestępców, godząc się na zapłatę żądanego okupu (kazus szpitalu w New Jersey).

Wśród cyberataków z udziałem ransomware na sektor ochrony zdrowia, jakie miały miejsce w ostatnim czasie można wskazać również na incydent w amerykańskim centrum medycznym University of Vermont Medical Center (VMC), niemieckim Instytucie Roberta Kocha (główny podmiot odpowiedzialny za walkę z COVID-19 w tym kraju), niektórych szpitalach w prowincji Quebec (Kanada) oraz 400 innych amerykańskich placówkach medycznych.

Jednak najbardziej dramatyczna w skutkach operacja z udziałem ransomware miała miejsce w Szpitalu Uniwersyteckim w Düsseldorfie. W wyniku działań hakerów doszło do zablokowania systemów i placówka nie mogła przyjmować osób potrzebujących natychmiastowej pomocy. Doprowadziło to do śmierci kobiety, która wymagała pilnej opieki lekarzy. Ze względu na zablokowanie komputerów oraz sieci pacjentka musiała zostać przewieziona do szpitala w innym mieście. Okazało się to dla niej śmiertelnym zagrożeniem.

Czytaj też: CISA: Alert dla służby zdrowia. Cyberprzestępcy nie odpuszczają szpitalom