**GandCrab zaatakował kolejną firmę medyczną**

**Firma świadcząca usługi w zakresie rozliczeń medycznych, z siedzibą w Massachusetts, powiadomiła pacjentów o naruszeniu swoich zasobów informacyjnych. Przyznała, że hakerzy mogli ujawnić ich dane. Atak przeprowadzono cieszącym się złą sławą oprogramowaniem szantażującym GandCrab.**

*- W ostatnich latach hakerzy szczególnie gustują w atakach na instytucje opieki zdrowotnej i ich zaplecze. Infekują systemy IT oprogramowaniem szantażującym (ransomware) lub wstrzykują złośliwy kod, mający za zadanie kradzież danych, które następnie wykorzystywane są w przyszłych oszustwach* - **tłumaczy Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe**.

Jedno z najnowszych doniesień o infekcji ransomware pochodzi od firmy medycznej Doctors’ Management Service, Inc. (DMS), która padła ofiarą ataku oprogramowaniem GandCrab.

Do naruszenia doszło, zgodnie z zawiadomieniem DMS uzyskanym przez databreaches.net, w kwietniu 2017 r. Natomiast odkryto je dopiero w grudniu ubiegłego roku, kiedy to wykorzystując protokół RDP hakerzy wdrożyli oprogramowanie ransomware na słabo chronionej stacji roboczej. Przeprowadzone później dochodzenie ujawniło, że napastnicy wykorzystali GandCrab, oprogramowanie szantażujące czyniące w ostatnich czasach największe szkody.

DMS odmówił zapłaty żądanego okupu i odzyskał dane z kopii zapasowych. Ponieważ nie można wykluczyć, że hakerom udało się również wykraść informacje o pacjentach, firma powiadomiła o zdarzeniu wszystkich, którzy mogli zostać nim dotknięci. Jeżeli atakujący skopiowali dane przed ich zaszyfrowaniem, byliby w posiadaniu imion i nazwisk, adresów, dat urodzenia, numerów ubezpieczenia społecznego, numerów prawa jazdy, informacji dotyczących ubezpieczenia zdrowotnego oraz informacji medycznych, w tym poufnych danych diagnostycznych.

Osoby, które otrzymały powiadomienie od DMS, zachęca się do skorzystania z oferowanej przez firmę bezpłatnej usługi monitorowania kredytu. Ponieważ jednak monitorowanie kredytu nie jest równoważne ochronie przed oszustwami, zainteresowanym osobom zaleca się uważne śledzenie wyciągów bankowych, pod kątem wystąpienia jakichkolwiek nieprawidłowości.