Bitdefender

Swatting – nowa metoda cyberprzestępców wykorzystujących ransomware

10.01.2024

Cyberprzestępcy korzystający z ransomware rozszerzyli swój zestaw narzędzi do specyficznego szantażu i nie polegają już wyłącznie na blokowaniu krytycznych systemów oraz grożeniu ujawnieniem skradzionych danych. Niektórzy napastnicy uciekają się obecnie swattingu, czyli wysyłania organów ścigania do domów ofiar pod fałszywym pretekstem, co stanowi kolejne zagrożenie dla osób poszkodowanych przez gangi ransomware.

Ewolucja ataków ransomware

Jeszcze kilka lat temu ataki ransomware polegały na blokowaniu danych ludzi i firm. Napastnicy prosili następnie o pieniądze w zamian za klucze umożliwiające ich odblokowanie. W końcu przestępcy zorientowali się, że jeśli mają dostęp do wdrażania oprogramowania ransomware, mogą

również kraść dane i wykorzystywać je jako dźwignię do ataków na inne firmy.

Ransomware przechodzi obecnie kolejny etap swojej ewolucji, ponieważ przestępcy zaczęli grozić ofiarom swattingiem. W przypadku swattingu do domu ofiary wysyłane są organy ścigania pod fałszywym pretekstem; zwykle zgłasza się im, że pod danym adresem przebywa ktoś uzbrojony i niebezpieczny. Czasami skutkiem swattingu jest śmierć niewinnych ludzi z rąk organów ścigania.

„Fed Hutchinson Cancer Center wiedział o cyberprzestępcach grożących atakiem i natychmiast powiadomił FBI i policję w Seattle, która powiadomiła lokalną policję" – powiedział rzecznik The Register. „W ramach dochodzenia w sprawie incydentu związanego z cyberbezpieczeństwem FBI zbadało również tego typu zagrożenia.

Pacjenci zagrożeni atakami ransomware

W listopadzie 2023 r. ośrodek onkologiczny im. Freda Hutchinsona stał się celem ataku, ponieważ przestępcy uzyskali dostęp do sieci klinicznej i uzyskali informacje o pacjentach. Obecnie przestępcy uciekają się do grożenia pacjentom swattingiem, co stanowi incydent związany z cyberbezpieczeństwem i przenosi się na inny poziom ze znacznie poważniejszymi konsekwencjami.

To nie pierwszy raz, kiedy przestępcy atakują pacjentów lub klientów firm. Kilka lat temu operatorzy oprogramowania ransomware zaczęli grozić klientom kancelarii prawnych, w których doszło do naruszeń,

wyciekiem zapieczętowanych dokumentów.

„Swatting to kolejna niebezpieczna taktyka należąca do repertuarów bezwzględnych cyberprzestępców. Jest ona szczególnie perfidną formą szantażu, ponieważ większość użytkowników sieci nie chce mieć do czynienia z uzbrojonym kordonem służb specjalnych. Dlatego to niezwykle istotne, aby nie dopuścić do zainfekowania naszego systemu przez złośliwe oprogramowanie. W tym celu należy zawsze korzystać ze skutecznego systemu antywirusowego, unikać pirackich treści i zachować szczególną ostrożność, gdy otrzymamy niespodziewane wiadomości e-mail” – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/swatting-nowa-metoda-cyberprzestepcow-wykorzystujacych-ransomware/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 02.01.2024
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia

bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.