Bitdefender

Cyberprzestępcy nie mają Twoich kompromitujących filmów. Nie daj się szantażować

02.08.2024

Grożenie komuś udostępnieniem obrazów i filmów z zainfekowanego urządzenia jest powszechną taktyką przestępczą od lat. Można by pomyśleć, że nie ma szans, aby ktoś w to uwierzył. Fakt, że wciąż mamy do czynienia z tym absurdalnym twierdzeniem przestępców, oznacza, że to działa i że jest wystarczająco dużo ofiar, aby uzasadnić większą ostrożność.

Próby wyłudzeń i szantaże

Dawno temu cyberprzestępcy mieli znacznie łatwiejsze zadanie w kontekście włamywania się do urządzeń, zwłaszcza komputerów. Przejęcie kontroli nad kamerą internetową było znacznie łatwiejsze i zazwyczaj wiązało się z oszukaniem ludzi, aby sami zainstalowali złośliwe oprogramowanie.

Technicznie rzecz biorąc, ten typ złośliwego oprogramowania nadal istnieje, ale rozwiązania zabezpieczające są znacznie bardziej powszechne. Nakłonienie ludzi do dobrowolnej instalacji złośliwego oprogramowania wymaga teraz wielu socjotechnik, a przestępcy prawdopodobnie wykorzystają ten czas i wysiłek na bardziej lukratywne ataki. Na przykład oszukanie ludzi, aby zainstalowali trojana bankowego, który daje hakerom bezpośredni dostęp do aplikacji bankowych, może wyrządzić znacznie więcej szkód.

Włamanie się do urządzeń jest naprawdę trudne

Na przestrzeni lat jedną rzeczą, która się zmieniła, jest łatwość naruszenia bezpieczeństwa urządzenia bez świadomego lub nieświadomego udziału użytkownika. Obecnie, aby przekonać użytkownika do zainstalowania aplikacji innej firmy na Androidzie lub oszukać użytkownika Apple, aby udostępnił swoje dane uwierzytelniające w ataku phishingowym, potrzebne są złożone techniki inżynierii społecznej.

To powinna być pierwsza linia obrony przed atakami, w których przestępcy twierdzą, że mają dostęp do Twojego urządzenia. Ten rodzaj oszustwa ma nazwę: sextortion.

Podstawowy przekaz jest prosty, a przestępcy nie przebierają w słowach. Zainstalowali złośliwe oprogramowanie na Twoim urządzeniu, telefonie lub komputerze (nie podają szczegółów) i nagrali Cię w kompromitującej pozie. Grożą, że ujawnią nagrania tylko wtedy, gdy nie otrzymają zapłaty, Cyberprzestępcy nie mają Twoich kompromitujących filmów. Nie daj się szantażować

zwykle w Bitcoinach.

Oczywiście cyberprzestępcy, nie mają żadnego nagrania z Tobą, a Twoje urządzenie nie zostało naruszone. Oszuści wiedzą, że tego typu wiadomości e-mail mogą trafić do skrzynki odbiorczej kogoś, kto niewiele wie o cyberbezpieczeństwie, lub nie wie, że to, co przestępcy piszą w wiadomości e-mail, jest wysoce nieprawdopodobne.

Przestępcy próbują być przekonujący

Podobnie jak wszystkie ataki, e-maile sextortion znacznie ewoluowały na przestrzeni lat. Przed pojawieniem się narzędzi takich jak ChatGPT, tekst był pisany zniekształconym angielskim i łatwo było stwierdzić, że prawdopodobnie jest to oszustwo. Niestety aktualne narzędzia do generowania tekstów dają możliwość oszustom tworzenia całkowicie poprawnych tekstów.

Inną taktyką, która zapewni atakującym większą wiarygodność, jest wstawienie hasła, którego potencjalne ofiary używały w przeszłości. Z badań Bitdefender wynika, że około 30 do 40 procent osób używa tego samego hasła na wielu kontach online. Ponadto duża część tych użytkowników będzie również używać tego samego hasła nawet po powiadomieniu o naruszeniu danych.

Jeśli użytkownik zobaczy swoje hasło w wiadomości e-mail, w której ktoś grozi ujawnieniem prywatnych filmów, może to być dla niego wystarczającym powodem, aby uwierzyć, że atakujący rzeczywiście mają dostęp do jego urządzenia.

Niestety przestępcy wykorzystują hasła z naruszeń danych, aby nadać wiarygodności swoim e-mailom, wiedząc, że wielu użytkowników się nie domyśli.

Ochrona Twojego życia prywatnego przed oszustwami typu sextortion

Pierwsza linia obrony jest również najważniejsza. Użytkownicy wiedzący o istnieniu oszustwa typu sextortion dają im ogromną władzę. Łatwo je rozpoznać, a usunięcie wiadomości e-mail jest bardzo proste.

Niektóre organizacje mogą mieć dedykowane filtry, które mogą chronić użytkowników, ale co z użytkownikami, którzy nie mają w pełni zabezpieczonego firmowego e-maila?

„Kluczowym elementem ochrony przed phishingiem i oszustwami związanymi z szantażem jest korzystanie ze skutecznego systemu antywirusowego wyposażonego w moduł antyphishingowy. Warto także zapamiętać, aby nigdy nie przelewać środków oszustom, którzy twierdzą, że mają kompromitujące cię materiały. Najprawdopodobniej kłamią, a nawet jeśli nie, to nie masz żadnej pewności, że po wpłacie okupu faktycznie usuną kompromitujące Cię zdjęcia, lub filmy” – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/cyberprzestepcy-nie-maja-twoich-kompromitujacych-filmow-nie-daj-sie-szantazowac/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 02.08.2024

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.