Hakerzy ukradli prawie 26 milionów danych logowania

15 czerwca 2021

Według dostawcy cyberbezpieczeństwa NordLocker hakerzy używający niestandardowego szkodliwego oprogramowania typu trojan ukradli prawie 26 milionów danych logowania – e-maili lub nazw użytkownika i powiązanych haseł – z prawie miliona stron internetowych w ciągu dwóch lat, w tym z Amazona, Facebooka i Twittera.

Według badań przeprowadzonych przez NordLocker we współpracy z firmą zewnętrzną specjalizującą się w naruszaniu danych, złośliwe oprogramowanie przeniknęło do ponad 3 milionów komputerów z systemem Windows w latach 2018-2020, przy czym cyberprzestępcy pozyskali około 1,2 terabajtów danych osobowych. 26 milionów skradzionych danych logowania pochodziło z dwunastu różnych typów stron internetowych, w tym mediów społecznościowych, gier online i usług e-mail. Były wśród nich takie marki jak Google (1,54 mln), Facebook (1,47 mln), Amazon (0,21 mln), Apple (0,13 mln), Netflix (0,17 mln) i PayPal (0,15 mln).

Oprócz danych logowania skradzione dane obejmują 1,1 miliona unikalnych adresów e-mail, ponad 2 miliardy plików cookie i 6,6 miliona plików, które użytkownicy przechowywali na swoich komputerach stacjonarnych i w folderach pobierania. Skradzione pliki cookie, które w niektórych przypadkach mogą umożliwiać dostęp do kont online ofiary, zostały podzielone na pięć grup: rynek online, gry online, witryna do udostępniania plików, media społecznościowe i usługi przesyłania strumieniowego wideo. Miliardy skradzionych ciasteczek były powiązane z takimi serwisami jak YouTube (17,1 mln), Facebook (8,1 mln), Twitter (5,2 mln), Amazon (3,5 mln), MediaFire (3,2 mln) i eBay (2 mln).

Szkodliwe oprogramowanie atakowało głównie przeglądarki internetowe w celu kradzieży danych, przy czym trzy największe źródła oprogramowania dla skradzionych wiadomości e-mail/nazw użytkownika oraz haseł to Google Chrome (19,4 mln), Mozilla FireFox (3,3 mln) i Opera (2 mln). Oprócz kradzieży plików oprogramowanie wykonywało również zrzuty ekranu zainfekowanych komputerów i zdjęć za pomocą kamery internetowej. Szkodliwe oprogramowanie było przesyłane za pośrednictwem poczty e-mail i pirackiego oprogramowania, w tym nielegalnych wersji Adobe Photoshop 2018 i szeregu zkrakowanych gier.

Źródło oryginalne: ZeroHedge.com
Źródło polskie: PrisonPlanet.pl