Czy Twoje hasła są przechowywane w bezpieczny sposób

ID artykułu: 58077 / 2264

URL: http://www.publikuj.org/58077

W 2019 roku znacząco wzrosło wykorzystywanie szkodliwego oprogramowania stworzonego w celu przechwytywania danych cyfrowych klientów programów wykradających hasła. Z danych firmy Kaspersky wynika, że liczba użytkowników stanowiących cel takich szkodników zwiększyła się z poniżej 600 000 w pierwszej połowie 2018 r. do ponad 940 000 w tym samym okresie w 2019 r. Szkodliwe oprogramowanie kradnące hasła stanowi główną broń w zestawie narzędzi cyberprzestępców wykorzystywanych do naruszania prywatności użytkowników. Szkodniki takie stosują różne metody w celu przechwytywania danych bezpośrednio z przeglądarek internetowych użytkowników. Zwykle są to wrażliwe informacje obejmujące dane umożliwiające dostęp do kont online oraz informacje finansowe, takie jak zapisane hasła, dane autouzupełniania oraz zapisane dane dot. kart płatniczych.

Ponadto niektóre rodziny tego rodzaju programów służą do kradzieży ciasteczek przeglądarki, plików użytkownika z określonej lokalizacji (na przykład z pulpitu), jak również plików aplikacji, takich jak komunikatory internetowe.

W ciągu minionych sześciu miesięcy badacze z firmy Kaspersky wykryli wysoki poziom aktywności programów wykradających dane w Europie oraz Azji. Ich celem byli najczęściej użytkownicy w Rosji, Indiach, Brazylii, Niemczech oraz Stanach Zjednoczonych.

Jednym z najszerzej rozprzestrzenionych trojanów wykradających hasła był wielofunkcyjny program Azorult, wykryty na komputerach ponad 25% wszystkich użytkowników, którzy w analizowanym okresie zetknęli się trojanami kradnącymi hasła.

Współcześni konsumenci wykazują coraz większą aktywność online, wykorzystując internet w celu wykonywania wielu codziennych zadań. W ten sposób ich profile cyfrowe wypełniają się coraz większą ilością danych, a sami stają się lukratywnym celem przestępców, którzy mogą w różny sposób zarobić na nich pieniądze. Jednak bezpieczne przechowywanie haseł i danych uwierzytelniających pozwala korzystać z ulubionych serwisów online bez obaw o prywatne informacje. Ponieważ ostrożności nigdy za wiele, warto dodatkowo zainstalować skuteczne rozwiązanie zabezpieczające powiedział Aleksander Jeremin, badacz ds. cyberbezpieczeństwa w firmie Kaspersky.

Porady bezpieczeństwa Eksperci z firmy Kaspersky sugerują stosowanie się do poniższych zaleceń w celu zapewnienia bezpieczeństwa swoim hasłom oraz innym danym uwierzytelniającym:

Nie ujawniaj znajomym ani rodzinie swoich haseł oraz informacji osobistych, ponieważ w ten sposób mogą stać się podatne na szkodliwe oprogramowanie. Nie udostępniaj ich ponadto na forach ani w kanałach mediów społecznościowych.

Zawsze instaluj aktualizacje oraz łaty bezpieczeństwa dla posiadanych produktów w celu zapewnienia ochrony przed najnowszym szkodliwym oprogramowaniem oraz zagrożeniami.

Zacznij korzystać z niezawodnego rozwiązania zabezpieczającego, takiego jak Kaspersky Password Manager, które umożliwia bezpieczne przechowywanie haseł oraz informacji osobistych, w tym paszportu, prawa jazdy oraz kart bankowych.

Więcej informacji odnośnie tego, w jaki sposób cyberprzestępcy wykorzystują szkodliwe oprogramowanie w celu kradzieży haseł oraz innych poufnych informacji, znajduje się na stronie https://r.kaspersky.pl/V Lmdy.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky jako źródła.

Wszystkie informacje prasowe są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00

Aktywacja: 23/07/19 14:04, odsłony: 94