Zapisywanie haseł w przeglądarce – dlaczego to błąd?

Istnieją różnego rodzaju oprogramowania do wykradania haseł bezpośrednio z przeglądarek. Najczęściej są one publikowane na różnych forach Darknetu.

Z tego artykułu dowiesz się w jaki sposób chronić się przed takimi podobnymi atakami.

Jak przebiega wykradanie haseł z przeglądarek?

Obecnie mamy coraz więcej ataków na różne popularne korporacje. Przykładem jest firma AhnLab (specjalizująca się w sprawach bezpieczeństwa np. dystrybucji oprogramowania antywirusowego)

Użytym narzędziem do przeprowadzenia takiego ataku był malware „Redline Stealer", ale mogą też inne tego typu oprogramowania, które działają podobnie.

Takie programy są oczywiście możliwe do kupienia w forach darknetu od marca 2020 r. Mają zdolność do wykradania danych z przeglądarki, nie tylko dane uwierzytelniające, ale również dane kart płatniczych.

Malware tego typu może wykradać dane z przeglądarek w oparciu o silnik Chromium oraz Gecko.

Dane logowania po zapamiętaniu ich w przeglądarce lądują w pliku SQLLite o nazwie *Login Data.* Plik ten znajduje się w różnych miejscach w zależności od

systemu lub przeglądarki np. na komputerach z Windowsem i dla przeglądarki Chrome znajdziemy go w katalogu *C:|Users|<NAZWA UŻYTKOWNIKA>|AppData|Local|Google|Chrome|User Data|Default*

Jak działa malware Redline Stealer?

To malware, który jak już wspominaliśmy wykrada dane z przeglądarek, pracujące na silnikach Chrome oraz Gecko.

Sam malware potrafi być rozpowszechniany pod różnymi postaciami oprogramowania np. jako do edycji obrazów czy dźwięków.

Cena tego narzędzia waha się między 150-200 USD, mimo iż czasami można trafić dane użytkowników zupełnie za darmo.