Szarek Mariusz

Abstract

Phishing is one of the most common and most dangerous attacks in cyberspace - which has been shown in this dissertation based on Polish and international statistics of computer security teams. A thorough understanding of how phishing works, what are its components, and how many attack phases the entire process consists of will allow you to identify and indicate those elements that will effectively identify it. The purpose of this dissertation was a thorough analysis of a phishing attack (included in Chapter I), and

a comparison of the detection methods used so far (Chapter II). The techniques and methods used by the attackers presented in Chapter I were used to show in Chapter III the indicators (which are the author's proposal) that characterize malicious emails. Chapter IV contains a proposal of a method that allows reading the described indicators from the message, their proper coding (including using machine learning), and then using the ML module to determine whether a given message can be a phishing attack. The conducted research showed that machine learning methods can recognize a phishing attack, also based on a previously unknown pattern.

.

Szarek Mariusz

Szarek Mariusz

Streszczenie

Phishing jest jednym z najczęstszych i najgroźniejszych ataków w cyberprzestrzeni - co zostało w niniejszej rozprawie ukazane na bazie polskich i międzynarodowych statystyk zespołów bezpieczeństwa komputerowego. Dokładne zrozumienie jak działa phishing, jakie są jego elementy składowe, z ilu faz ataku składa się cały proces pozwoli na określenie i wskazanie tych elementów, które skutecznie pozwolą na jego identyfikacje. Celem niniejszej rozprawy było dokładna analiza ataku phishingowego (zawarta w rozdziale I), porównanie dotychczas wykorzystywanych metod detekcji (Rozdział II). Przedstawione w Rozdziale I techniki i metody stosowane przez atakujących posłużyły do wykazania w Rozdziale III wskaźników (będących autorską propozycją), jakimi charakteryzują się wiadomości email o złośliwym charakterze. Rozdział IV zawiera propozycję metody pozwalającej na odczytanie z wiadomości opisanych wskaźników, właściwe ich zakodowanie (w tym z wykorzystaniem uczenia maszynowego), a następnie za pomocą modułu ML określenie czy dana wiadomość może być atakiem phishingowym. Przeprowadzone badania wykazały, że metody uczenia maszynowego mogą rozpoznawać atak phishingowy, bazujący również na nieznanym wcześniej wzorcu.

Szarek Mariusz