Streszczenie rozprawy doktorskiej „Budowanie mechanizmu obrony przed dedykowanymi kampaniami phishingowymi”

AUTOR:
mgr inż. Mariusz SZAREK
PROMOTOR:
dr hab. inż. Ryszard ANTKIEWICZ, profesor WAT

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.