CZARNY PIĄTEK: WIELKA OKAZJA DLA CYBERPRZESTĘPCÓW

Polując na okazję w ramach Czarnego Piątku, sam możesz stać się okazją dla hakerów. Cyberprzestępcy zacierają ręce i przygotowują się na wielką wyprzedaż.

Według badaczy z firmy Kaspersky szczególną ostrożność podczas dokonywania zakupów online należy zachować w przypadku sklepów oferujących odzież, obuwie, prezenty, zabawki i biżuterię.

Firma przeprowadziła analizę zagrożeń związanych z czarnopiątkowymi wyprzedażami, w tym botnetów służących do rozprzestrzeniania trojanów bankowych, czyli szkodliwego oprogramowania wykorzystywanego do kradzieży danych uwierzytelniających oraz informacji finansowych użytkowników.

Zidentyfikowano 15 rodzin szkodliwego oprogramowania, których celem było łącznie 91 stron handlu elektronicznego oraz aplikacji mobilnych na całym świecie.

Jak podano, operatorzy botnetów finansowych skupiali się na towarach konsumpcyjnych, takich jak odzież, biżuteria czy zabawki – klienci 28 sklepów internetowych z tej kategorii stanowili cel szkodliwego oprogramowania. Na dalszym miejscu znalazł się segment rozrywki, obejmujący filmy, muzykę oraz gry. Cyberprzestępcy celowali także w klientów usług związanych z turystyką, takich jak serwisy prowadzące sprzedaż biletów komunikacyjnych, usługi taksówkowe czy hotele.

Hakerzy próbują zdobyć dane uwierzytelniające użytkowników sklepów internetowych, gdyż z takimi kontami czesto połączone są dane dotyczące kart płatniczych lub szczegóły kart programów lojalnościowych. Konta użytkowników zawierają wiele informacji, mogących zostać wykorzystanych do dalszych ataków, jak np. historia zakupów, informacje osobowe czy adresy dostaw.

Eksperci firmy Kaspersky zalecają, by unikać zakupów na stronach, które wydają się podejrzane lub nie działają sprawnie, nawet jeśli oferują doskonałe okazje. Nie należy klikać nieznanych odsyłaczy otrzymanych niespodziewanie w wiadomościach e-mail lub za pośrednictwem portali społecznościowych, nawet od znanych osób. Apelują też, by dokładnie sprawdzać adres e-mail nadawcy, i jeśli nie zawiera oficjalnej domeny strony internetowej marki, nie klikać odsyłacza.

O ile jest to możliwe, należy wybierać serwisy przetwarzania płatności wykorzystujące wieloskładnikową autoryzację zakupów.

Zalecają też, by na urządzeniu, z którego dokonywane są zakupy, korzystać z wyspecjalizowanego rozwiązania zabezpieczającego z wbudowanymi funkcjami umożliwiającymi stworzenie bezpiecznego środowiska dla wszystkich transakcji finansowych.