WH WIADOMOŚCI HANDLOWE.PL

Grudniowy szał zakupowy przyciągnął przestępców – 3 najgroźniejsze cyberataki

data aktualizacji: 2019.01.03

W drugiej połowie grudnia skradziono dane ok. 2,2 mln klientów sklepu internetowego Morele.net. Wcześniej przeprowadzono atak z wykorzystaniem Paczkomatów InPost. Do oszustw często wykorzystywano także fałszywe strony bankowe.

Ponad 90 proc. polskich internautów robi zakupy w sieci. W okresie przedświątecznym agresywne akcje marketingowe i chęć zakupu prezentów w niższej cenie powodują, że tracimy ostrożność i jesteśmy bardziej podatni na ataki, często bardzo dobrze przygotowane psychologiczne. Cyberprzestępcy chętnie wykorzystują łatwowierność i roztargnienie konsumentów. Niestety nie zawsze na wysokości zadania stają też firmy, w tym sklepy internetowe, obciążone w grudniu do granic możliwości.

– Grudniowe przesilenie zakupowe sprzyja potencjalnym atakom. Wystarczy, że w natłoku zleceń ktoś w sklepie internetowym nie zaktualizuje systemów ochronnych, nie wyloguje się z systemu z danymi, czy otworzy podejrzaną wiadomość będącą próbą włamania. Jako konsumenci nauczyliśmy się już chronić swoje portfele, np. podczas zakupów w galerii handlowej, ale zapominamy o ochronie danych, które często są bardziej wartościowe niż to co mamy w portfelu – mówi Wojciech Gołębiowski, dyrektor zarządzający Veronym, firmy oferującej zabezpieczenia chmurowe w modelu

subskrypcji usługi.

Dane 2,2 mln osób skradzione ze sklepu internetowego

18 grudnia Grupa Morele, właściciel sklepu Morele.net, poinformowała o wycieku danych osobowych swoich klientów. Hakerzy uzyskali dostęp do imion i nazwisk, adresów e-mail, numerów telefonu, oraz zaszyfrowanych haseł. Właściciel sklepu uspokaja, że sytuacja została opanowana i zaleca ostrożność oraz… zmianę danych logowania. Skradzione informacje mogą zostać wykorzystane do prób wyłudzeń i do spamu reklamowego.

Niestety na horyzoncie jest też znacznie poważniejsze niebezpieczeństwo – jeśli zaszyfrowane hasła zostaną przez hakera odkodowane, to w połączeniu z adresami e-mail mogą zostać wykorzystane do ataków na innych stronach, bo wielu użytkowników używa tej samej kombinacji loginu i hasła w różnych miejscach w sieci. Właściciel sklepu poinformował, że wdrożył już odpowiednie procedury i środki bezpieczeństwa. Szkoda, że tak późno.

– Pojawiają się informacje, że haker lub hakerzy, którzy wykradli dane z wymienionego sklepu internetowego, zażądali okupu. To częsty sposób działania cyberprzestępców. Włamują się do komputerów firmy, przejmują dane lub blokują do nich dostęp, a następnie domagają się okupu. Jego wysokość zazwyczaj wielokrotnie przekracza koszt solidnej cyberochrony, a straty wizerunkowe, jakie w takim przypadku mają miejsce, są jeszcze większe i wymierne, bo skutkują np. utratą klientów -- mówi Wojciech Gołębiowski.

Twoja paczka czeka

W Polsce jest prawie 4500 Paczkomatów InPost. Firma dostarczyła w 2018 roku ponad 86 mln przesyłek, czyli o 52,5 proc. więcej niż rok wcześniej. W listopadzie i grudniu liczba przesyłek jest większa niż w pozostałych miesiącach. Tysiące osób codziennie dostaje e-maila informującego o zrealizowaniu dostawy zamówionego produktu. Zwykle są to wiadomości oczekiwane i pożądane. Wiedzą o tym oszuści, którzy podszywają się pod firmę InPost i popularną usługę Paczkomatów.

Zmasowana akcja hakerów wysyłających fałszywe e-maile na temat oczekującej na odbiór paczki miała miejsce w połowie października, jednak z mniejszym nasileniem podobne wiadomości były wysyłane prawdopodobnie do grudnia. Kliknięcie w podany link skutkowało pobraniem złośliwego załącznika z wirusem.

Fałszywa wiadomość wyglądała nieco inaczej niż prawdziwa, ale żółto-czarna kolorystyka e-maila, typowa dla popularnych skrzynek na przesyłki, była bardzo sugestywna, a liczba paczek, jakie zamawiamy w świątecznym okresie i radość, że wyczekiwany zakup już dotarł to połączenie, które wyłącza ostrożność.

Odbiorca oczekuje na płatność

Tworzone przez hakerów strony łudząco podobne do bankowych to bardzo poważne zagrożenie dla naszych pieniędzy. Zazwyczaj wykorzystywane są razem z fałszywymi e-mailami wyglądającymi zupełnie jak te od banku (kolorystyka, nazwa banku, układ treści, język). Wiadomości informują np. o konieczności ponowienia przelewu, który nie przeszedł lub został cofnięty przez bank, ewentualnie sugerują konieczność dopłaty brakującej kwoty np. za przesyłkę. W wiadomości jest aktywny link, który w rzeczywistości kieruje do fałszywej strony. Zalogowanie się na niej prowadzi do przejęcia przez oszustów danych logowania, które mogą oni wykorzystać do wejścia na rzeczywiste konto. Czasem kliknięcie w taki link powoduje ściągnięcie i instalację na komputerze oprogramowania

czytającego litery i cyfry wstukiwane na klawiaturze, np. podczas logowania do różnych stron i profili.

Źródło: https://www.wiadomoscihandlowe.pl/artykuly/grudniowy-szal-zakupowy-przyciagnal-przestepcow-3-,51652