

AKTUALNOŚCI

Trend Micro: socjotechnika na usługach oszustów w okresie przedświątecznym

12 grudnia 2008

NetWorld Online JM

Firma Trend Micro opracowała listę metod socjotechnicznych najczęściej stosowanych przez oszustów w okresie przedświątecznym. Za pomocą socjotechniki cyberprzestępcy starają się nakłonić swoje ofiary do kliknięcia łączników w rozsyłanych wiadomościach pocztowych, pobierania plików, czy wypełniania formularzy z poufnymi danymi osobowymi. Zgodnie z tradycją, w okresie przedświątecznym zwiększa się liczba użytkowników wyszukujących i kupujących różne produkty w internecie.

Według firmy, lista metod socjotechniki najczęściej wykorzystywanych przez oszustów internetowych przedstawia się następująco.

Poszukiwanie okazji - cyberprzestępcy wykorzystują fałszywe rabaty i promocje, aby skłonić ofiary do kliknięcia niebezpiecznych łączników lub podania poufnych informacji na podrabianych stronach internetowych. W ubiegłym roku koń trojański TROJ_AYFONE.A wyświetlał fałszywe reklamy i podrobioną stronę sklepu internetowego, w którym można było rzekomo kupić iPhone firmy Apple.

Fałszywe serwisy organizacji charytatywnych. Głośne katastrofy - huragany Katrina i Gustav, trzęsienie ziemi w Chinach, pożary lasów w Kalifornii - były wykorzystywane przez cyberprzestępców do wyludzenia rzekomej pomocy dla ofiar.

Elektroniczne kartki z życzeniami, które są często wykorzystywane przez cyberprzestępców jako zachęty do kliknięcia niebezpiecznego łącznika w fałszywej wiadomości.

Fałszywe reklamy i promocje. Reklamy umieszczane na często odwiedzanych stronach internetowych mogą inicjować pobranie szkodliwego oprogramowania lub wyludzać dane osobowe przez pozornie nieszkodliwe ankiety.

Fałszywe wyniki wyszukiwania niektórych ciągów znaków, sfalszowane za pomocą złośliwych skryptów, które mogą w konsekwencji doprowadzić do pobrania szkodliwego oprogramowania, phishingu lub kliknięcia niebezpiecznego adresu URL. W roku ubiegłym fałszywe wyniki, które kierowały do różnych szkodliwych programów, dawało wyszukiwanie wyrażenia "christmas gift shopping". W tym roku wyniki wyszukiwania tekstu "halloween costumes" kierowały do fałszywego oprogramowania antywirusowego.

Zainfekowane popularne serwisy internetowe, które są bardzo groźne, ponieważ są uważane przez użytkowników za bezpieczne i godne zaufania. Wykorzystując popularne serwisy o dużym natężeniu ruchu, cyberprzestępcy mogą w tym czasie zainfekować więcej użytkowników.

Phishing w handlu internetowym. Serwis eBay - najpopularniejszy internetowy sprzedawca detaliczny w ubiegłym roku - był jednocześnie także na czele listy serwisów internetowych najczęściej wykorzystywanych do phishingu.

Spam w postaci rzekomych wiadomości od popularnych firm kurierskich z informacjami o niedostarczonych przesyłkach. Do wiadomości jest dołączany plik, który wygląda jak list przewozowy. Znane są przykłady działań tego typu z wykorzystaniem firm kurierskich UPS i FedEx.

Fałszywe faktury - wiadomość poczty elektronicznej z poleceniem otwarcia i wydrukowania faktury przysłanej w załączniku, która jest plikiem zawierającym konia trojańskiego. Celem tego rodzaju ataków są osoby często dokonujące zakupów online, przyzwyczajone do otrzymywania takich rachunków.

Regulamin i polityka prywatności
Kontakt



04-204 Warszawa ul. Jordanowska 12
tel.: (+48 22) 321 78 00 fax: (+48 22) 321 78 88
© copyright 2008 IDG Poland SA