Społeczność hakerów

10 listopada 2009

Czym są portale społecznościowe, nie trzeba nikomu wyjaśniać. Dziś niemal każdy użytkownik Internetu ma swój profil na Naszej – Klasie, Goldenline, Facebooku czy BLIP-ie.

JAK DZIAŁAJĄ HAKERZY?

W ostatnich miesiącach media niemal codziennie informowały o nowych atakach phishingowych, dokonywanych na użytkowników portali społecznościowych. Schemat działań cyberprzestępców zawsze wygląda tak samo – poszczególne osoby otrzymują wiadomość, wysyłaną często dla potwierdzenia jej autentyczności z centrum pomocy portalu, zawierającą link lub buton przekierowujący na fałszywą stronę, łudząco podobną do strony startowej , na której użytkownik, w celu aktualizacji konta, proszony jest do podania swojego loginu i hasła. Spełnienie tych warunków jest jednoznaczne z przekazaniem swojego profilu hakerom oraz, niejednokrotnie, pobraniem trojana, który wykradnie dane finansowe. Hakerzy, którzy działają na serwisach społecznościowych, wykorzystują rozmaite narzędzia, a każdy kolejny atak odznacza się coraz większą pomysłowością i precyzją. Wykorzystując np. telnet, są w stanie wysłać wiadomość pocztową niemal z każdej domeny. Praktycznie więc, informacja przychodząca od „administratora serwisu" może okazać się elementem skrupulatnie przemyślanego ataku phishingowego.

ATAKI NA PORTALE SPOŁECZNOŚCIOWE

Nie tak dawno użytkowników Twitera zaskoczył kolejny wymyślny atak hakerów –w komentarzach zaczęły pojawiać się informacje o tym, jak łatwo i szybko można zarobić, korzystając z Google. Link zamieszczony we wpisach odsyłała do fake'owej strony www. „Chociaż formalnie nowa witryna nie wymagała podania swojego loginu czy hasła, to jednak już samo kliknięcie linku mogło

skutkować pobraniem program szpiegującego, jaki hakerzy często umieszczają na tego typu serwisach” tłumaczy Tomasz Zamarlik z G Data Software.

Zgoła inną niespodzianką zaskoczył swoich użytkowników Facebook, gdzie ilość zarejestrowanych profili, przekroczyła w zeszłym miesiącu liczbę 300 milionów. Hakerzy włamując się na konta zalogowanych osób, rozesłali do ich znajomych wiadomości zawierające link do zainfekowanej złośliwym oprogramowaniem strony. Chociaż administratorzy serwisu starają się błyskawicznie reagować na niepokojące sygnały, to jednak często, jedynym co mogą zrobić, jest resetowanie kont shakowanych użytkowników. Nie jest natomiast możliwe prowadzenie jakiejkolwiek bazy danych, zawierającej nr IP czy inne informacje, które umożliwiłyby zidentyfikowanie cyberprzestępców. Stąd, łatwo przewidzieć, że tego typu działania będą się jeszcze powtarzać. „Osoby, z których kont generowane są tego typu wiadomości, oraz odbiorcy fałszywych linków powinni natychmiastowo zmienić hasło. Takie informacje to pierwszy sygnał, że z naszym profilem dzieje się coś złego” wyjaśnia Tomasz Zamarlik.

Przedstawiony powyżej przykład to jedna z bardziej wymyślnych form ataku. Wiadomość generowana rzekomo przez administratorów sieci Facebook, została rozesłana do 750 tyś użytkowników. E–mail wysyłany był z adresu service@facebook.com, co jeszcze bardziej miało potwierdzić jego autentyczność. Zamieszczone w załączniku hasło, okazało się być Trojanem, który instalował się na komputerze jako plik z rozszerzeniem .exe, zmieniając niektóre aplikacje systemowe na komputerze ofiary. Podobne działania przeprowadzane są również na innych portalach społecznościowych. W marcu tego roku, podobny atak został przeprowadzony na użytkowników portalu MySpace, tym razem z wykorzystaniem wirusa Koobface. Na ataki hakerów narażeni są również użytkownicy portalu Nasza-Klasa. Wybierając odpowiednie grupy tematyczne, hakerzy mogą wysyłać SPAM do zdefiniowanego wcześniej grona osób.

JAK UNIKNĄĆ KRADZIEŻY KONTA?

Monitorowanie sieci botnet, za pomocą których hakerzy wysyłają stworzony przez siebie SPAM, nie zawsze przynosi dobre rezultaty. Jak podają naukowcy z G Data Software, bardzo często zanim administratorzy konta zauważą, że dzieje się coś złego, wiadomość jest już wygenerowana do blisko 700 tyś osób, z których większość, nie mając pojęcia o zagrożeniu, zaloguje się na fałszywą stronę. „Zalecane przez właścicieli portali środki ostrożności nie są wystarczające. Zaledwie niewielki odsetek osób sprawdza adres domeny, na jaki przekierowuje fałszywa strona. Dlatego warto swój komputer zabezpieczyć programem antywirusowym – chociaż, co prawa, nie uchroni on nas przed podawaniem naszych danych, to jednak zapobiegnie zainstalowaniu się na komputerze złośliwego oprogramowania” wyjaśnia Tomasz Zamarlik.

TRADYCYJNE FORMY ATAKÓW WCIĄŻ SĄ MODNE

Często wina za dokonywanie ataków leży także po stronie administratorów serwisów społecznościowych. Niewłaściwe zabezpieczenie danych użytkowników, w tym odstąpienie od szyfrowania haseł, to jedna z głównych przyczyn wycieku haseł zarejestrowanych Internautów. Takie informacje, chociaż nie dotyczą użytkowników bezpośrednio, mogą również wyrządzić wiele szkody. W zależności od tego, jakie dane udało się zdobyć hakerom, mogą oni na kosz ofiary zrobić zakupy w sklepie online, zalogować się na konto w e-banku, czy rozsyłać SPAM do innych użytkowników sieci.

Autor: Dariusz Ptaszek
Źródło: iThink.pl