Robak Rainbow wykorzystał do rozprzestrzeniania się słaby punkt Twittera, występujący podczas korzystania z serwisu bezpośrednio przez stronę www. Najechanie myszką na adres URL mogło powodować przekierowanie na inne strony, generowanie dziwnych komunikatów, wyświetlanie gigantycznych liter lub zasłoniętego tekstu, itp. Co 10 sekund rejestrowano nawet tysiąc infekcji. Luka w bezpieczeństwie umożliwiająca atak jest już w pełni załatana.

21. września br. firma Panda Security zaobserwowała pierwszą masową infekcję na popularnym serwisie społecznościowym Twitter. Wielu użytkowników było zdziwionych, widząc dziwny ciąg znaków na swoich profilach.

Przyczyną były błędy w kodzie Twittera, które doprowadziły do różnych niespodziewanych zdarzeń. Kiedy na stronie www.twitter.com użytkownicy najeżdżali myszką na tweety:

- złośliwy kod mógł być automatycznie rozsyłany do użytkowników obserwujących profil, powodując dalsze rozprzestrzenianie się szkodliwego tweeta;
- mogły pojawiać się dziwne komunikaty, ogromne litery, okna dialogowe z powitaniem, zasłonięte tweety itp.;
- osoby, które logowały się na swój profil mogły być przekierowywane na inne strony www.

Słaby punkt w kodzie umożliwiał działanie skryptu java, który otwierał szereg możliwości dla cyberprzestępców.

Luis Corrons, dyrektor techniczny Laboratorium PandaLabs powiedział: „Największym zagrożeniem była możliwość wykorzystania adresu URL stosowanego podczas ataku do zainfekowania komputera użytkownika. Jeśli poza dalszym rozsyłaniem kodu przestępca zamieściłby w kodzie strony odnośnik za pomocą technik „driver-by-download", moglibyśmy mówić o milionach potencjalnych ofiar".

Źródłem ataku wydaje się być konto na Twitterze o nazwie Rainbow. Tę samą nazwę nadano robakowi.

Pierwsze przypadki wstrzykiwania skryptu java do kodu strony były zwykłymi żartami, ale stopniowo ewoluowały do miana ataków. Wygląda na to, że obecnie przestępcy wykorzystują lukę w bezpieczeństwie do poważniejszych celów.

Programy typu klient obsługujące Twittera, które nie uruchamiają skryptu java, np. TweetDeck, były bezpieczne i pozwalały użytkownikom korzystać z serwisu bez ryzyka ataku „Rainbow". Ze strony Twittera można już korzystać bezpośrednio, ponieważ luka w bezpieczeństwie została załatana.

studio PRowokacja