

Żartobliwe aplikacje symulujące zarażenie trojanem zalewają sieć. Filmy „Paranormal Activity 2” i „Piątek Trzynastego” są obecnie najczęściej wykorzystywanymi do ataków BlackHat SEO w celu rozprzestrzeniania złośliwych kodów. Do tego spam rozsyłany w celu zbierania danych osobistych... Hakerzy jako wabik powszechnie wykorzystują grafiki związane ze świętem Halloween.

Wraz ze zbliżaniem się święta Halloween aplikacje, fałszywe strony internetowe, spam i trojany „przebierają się” by nabrać użytkowników. PandaLabs, laboratorium zabezpieczające firmy Panda Security, wykrywa tego typu ataki od sierpnia, jednak w ciągu ostatnich kilku dni ich liczba znacząco wzrosła. Stare techniki „wracają do życia” i wraz z nowymi odmianami oraz fałszywymi aplikacjami próbują nastraszyć użytkowników.

Halloweenowe psikusy sieją strach...

Pomimo, iż komputerowe żarty to nic nowego, w dniach poprzedzających Halloween ich liczba gwałtownie rośnie terroryzując użytkowników. W rzeczywistości takie aplikacje są niegroźne, ponieważ nie zawierają złośliwych kodów ani trojanów.

Zwykle docierają do komputera ofiary od kogoś z jej kontaktów, w formie halloweenowego pliku wideo lub internetowej kartki z życzeniami przesłanej w e-mailu lub przez sieć społecznościową. Po pobraniu i zainstalowaniu wyświetlają serię komunikatów i ekranów informujących użytkownika o zarażeniu komputera trojanem. Przykładowo jest to film flash, który symuluje usunięcie całej zawartości twardego dysku komputera, podczas gdy na ekranie pojawia się przerażająca czaszka. Strona, która rozpowszechnia ten psikus, oferuje film instruktażowy pokazujący, jak skonfigurować film, aby był on jeszcze bardziej realistyczny i straszny.

Na szczęście są to mistyfikacje. Komputer użytkownika nie zostaje zarażony złośliwym kodem, a jego twardy dysk nie zostaje sformatowany. Nie ma jednak wątpliwości, że można najeść się sporo strachu, sądząc, iż komputer został zniszczony!

Straszne filmy....

Do przeprowadzania ataków Blackhat SEO hakerzy wykorzystują znane produkcje Hollywood. W tym roku najpopularniejsze to „Paranormal Activity 2” oraz klasyk Halloween - „Piątek Trzynastego”. Atakujący wykorzystują modne tematy, aby pozycjonować złośliwe strony wśród najpopularniejszych wyników wyszukiwania. Gdy użytkownik wejdzie na zarażoną stronę na komputer zostaje pobrany trojan albo fałszywy antywirus. Te ataki wykorzystują nie tylko wzmianki o horrorach, ale także o wszystkim, co związane z tematem Halloween, np. zaproszenia na imprezy.

Spam na Halloween

Innym sposobem, w jaki hakerzy wywołują zamieszanie jest masowe rozsyłanie spamu o tematyce związanej z Halloween w celu skłonienia użytkowników do ujawnienia swoich danych osobistych albo zakupu fałszywych lub nielegalnych produktów. Często chodzi po prostu o zarabianie pieniędzy, gdyż wiele firm czerpie zyski z systemów pay-per-click.

Wskazówki

Jak zwykle najlepszą ochroną jest wiedza i zachowanie podstawowych środków ostrożności. Uważaj na wszelkie próby zrobienia niemiłego psikusa oraz prawdziwe zagrożenia, które starają się popsuć halloweenową zabawę.

Oto kilka wskazówek PandaLabs jak zapobiec zagrożeniu:

- Nie otwieraj emaili ani wiadomości z portali społecznościowych od nieznanych nadawców.
- Nie klikaj na żadne linki zawarte w emailach, nawet jeśli pochodzą z zaufanych źródeł. Lepiej wpisać adres bezpośrednio w okienku przeglądarki. Zasadę to warto stosować niezależnie od nadawcy, także w przypadku

wiadomości z Facebooka, Twittera i innych portali społecznościowych czy internetowych komunikatorów.

- Jeśli kliknąłeś na otrzymany link dokładnie przyjrzyj się witrynie na którą trafiłeś. Jeśli nie masz co do niej pewności zamknij przeglądarkę.
- Nie otwieraj plików z załącznika pochodzących z nieznanych źródeł. W szczególności uważaj na pliki, które w nazwie mają "Halloween".
- Nawet jeśli witryna internetowa wygląda wiarygodnie, ale sugeruje rozpoczęcie pobierania, powinieneś zachować szczególną podejrzliwość.
- Jeśli jednak ściągnąłeś i zainstalowałeś jakiekolwiek aplikacje, a teraz zaczynasz widzieć nietypowe wiadomości na swoim komputerze to prawdopodobnie został on zainfekowany złośliwymi kodami.
- Rób zakupy internetowe tylko na stronach, które cieszą się dobrą reputacją i oferują bezpieczne transakcje, szyfrując wszystkie informacje wpisywane na stronie. Aby sprawdzić, czy strona jest bezpieczna, poszukaj certyfikatu bezpieczeństwa w postaci małej żółtej kłódki obok paska narzędzi lub w prawym dolnym rogu ekranu.
- Nie korzystaj ze wspólnych lub publicznych komputerów do przeprowadzania transakcji lub operacji wymagających wpisania hasła lub innych danych osobistych.
- Zainstaluj skuteczne rozwiązanie zabezpieczające, zdolne wykrywać zarówno znane, jak i nowe odmiany zagrożeń.

Panda Security oferuje kilka bezpłatnych narzędzi do skanowania komputerów w poszukiwaniu zagrożeń, jak na przykład Panda Cloud Antivirus (<http://www.cloudantivirus.com/pl/>).

No i wesołego Halloween!

Panda Security