STÓJ | POMYŚL | POŁĄCZ

BOTNETY: FAKTY I DOBRE PRAKTYKI

CZYM SĄ BOTNETY?

Internet pozwala komunikować się z całym światem i czyni życie prostszym. Niestety, w sieci obecne są również osoby, które nie mają dobrych zamiarów i korzystają z niej, aby szkodzić innym. Popularnym rodzajem takiego szkodnictwa jest infekowanie podłączonych do Internetu urządzeń oprogramowaniem pozwalającym zdalnie je kontrolować.

Po udanym zarażeniu, urządzenie może stać się częścią botnetu – większej sieci zaatakowanych urządzeń, zdalnie kontrolowanych przez hakerów. Przestępcy korzystają z botnetów do osiągania korzyści majątkowych, rozsyłania spamu, infekowania kolejnych użytkowników, przeprowadzania ataków na strony internetowe i innych złośliwych działań. Pojedynczy botnet składa się przeważnie z kilkuset lub nawet kilku tysięcy rozproszonych po świecie urządzeń.

CO MOŻESZ ZROBIĆ?

Pomóż chronić siebie i innych użytkowników Internetu przed aktywnością botnetów i obecnych w sieci zagrożeń. Poznaj dobre praktyki kampanii STÓJ. POMYŚL. POŁĄCZ.

Zadbaj o aktualizacje: Pamiętaj by regularnie aktualizować oprogramowanie na posiadanych urządzeniach, szczególnie tych podłączonych do Internetu. System operacyjny na Twoim komputerze i smartfonie, program antywirusowy, aplikacje z których korzystasz - powinny być na bieżąco uaktualniane i używane w najnowszych dostępnych wersjach.

Twórz kopie zapasowe: Zabezpiecz efekty swojej pracy, muzykę, zdjęcia, cenne dokumenty. Regularnie wykonuj kopie zapasowe i przechowuj je w bezpiecznym miejscu.

Stwórz mocne hasło: Dobre hasło składa się z przynajmniej 12 znaków. Skup się na pozytywnych zdaniach i zwrotach, które łatwo zapamiętasz (np. „Kocham miasto muzyki”). Na wielu stronach internetowych, możesz przy wprowadzeniu hasła używać spacji.

Bądź świadomym użytkownikiem: Linki i załączniki w wiadomościach e-mail, spreparowane posty w mediach społecznościowych, a także reklamy - to częste metody używane przez przestępców w celu kradzieży danych. W momencie gdy wydają Ci się podejrzane, po prostu je zignoruj - nawet jeżeli źródło wygląda na zaufane.

Skanuj nośniki wymienne: Nie podłączaj do komputera urządzeń, których pochodzenie nie jest Ci znane. Pamięci USB, dyski zewnętrzne i inne nośniki danych, mogą być niebezpieczne (zainfekowane przez szkodliwe oprogramowanie). Zanim otworzysz ich zawartość, skorzystaj ze skanera antywirusowego.

Odwiedź https://stojpomyslpolacz.pl i dowiedz się więcej.