Grupa zwolenników otwartości Sieci i wolności słowa, zrzeszona w AnonOps, dołącza dobrowolnie do botnetu DDoSującego przeciwników WikiLeaks. W tym artykule postaram się wyjaśnić sprawę od strony technicznej.

Trochę historii

Jak podaje niebezpiecznik.pl, w związku z ujawnianiem coraz to większej ilości tajnych dokumentów USA, PayPal i MasterCard zablokowały konta WikiLeaks na które można było wpłacać dotacje. W odwecie Anonymous, odłam 4chan'a (znany także z atakowania antypiratów), postanowił znowu wziąć sprawy w swoje ręce i zorganizował we własnej sieci IRC akcję.

Metody nękania

Obecnym celem jest MasterCard. Zalecanym programem jest LOIC (Low Orbit Ion Cannon), wzbogacony o funkcję "ula" ("hive"), czyli zdalnej kontroli. Wystarczy wkleić adres serwera IRC i nazwę kanału, i nie trzeba się troszczyć o ręczne zmienianie celu. Kierujący atakiem ma uprawnienia operatora kanału i zmienia temat rozmowy ("topic"), który jest wysyłany do wszystkich uczestników. Dzięki temu LOIC wie na co kierować wrogie pakiety.

Ponieważ grupa chce zdobyć jak najwięcej zwolenników, powstają jeszcze prostsze w obsłudze programy, w tym działające w przeglądarce internetowej. Jeden z nich zamiast floodować stronę główną, spamuje pomoc techniczną MasterCard.

Oprócz brutalnego wysyłania pakietów używana jest także propaganda. Na przykład nawiązująca do znanej powieści Orwella, wykorzystująca Google Bomb - http://pastebin.com/Ud789JNv .

Jak działa LOIC?

Nas, informatyków (zarówno amatorów jak i kwalifikowanych), interesuje strona techniczna a nie ideologia. Pozwoliłem sobie poatakować bramę własnej sieci (która ma nginx) i przeanalizować całość w Wiresharku. Atak jest bardzo prosty i nie wymaga uprawnień root'a na komputerze-agresorze. W pętli następuje nawiązanie połączenia TCP, wysłanie tekstu i zamknięcie połączenia. Wszystko konwencjonalnie, bez sztuczek w stylu SYN flood, połączenie jest zwyczajnie nawiązywane i zwyczajnie kończone.

DDoS w JavaScript

To jest możliwe! W JS zostało zaprogramowane tworzenie kilkudziesięciu obiektów <img>, które są okresowo (np. co 0,1 sekundy) zmieniane. Aby uniknąć cache'owania, za każdym razem zmieniana jest ścieżka. Przeglądarka chcąc załadować obiekty podające się za obrazki, łączy się z serwerem-ofiarą i oczywiście go obciąża. Warto wiedzieć że taki atak może się odbywać bez świadomości użytkownika, wystarczy spreparować stronę internetową.

Co o tym sądzić?

Możesz podyskutować ze zwolennikami WikiLeaks w sieci IRC (anonops.eu). Ale do botnetu lepiej nie dołączać - może to być nielegalne.

Więcej informacji:

Uwaga! Wykonywanie instrukcji z poniższych linków, a nawet otwieranie niektórych, może być nielegalne! Używaj tylko w celach informacyjnych!

- http://www.anonops.eu/
- http://www.anonops.info/
- https://2wjsnwzoeiae4iyf.tor2web.org/
- http://bit.ly/fGHDib - instrukcja atakowania z użyciem LOIC
- http://pastehtml.com/view/1cb51vf.html - strona atakująca serwery poczty przy pomocy JavaScript. **Jeśli nie masz NoScript to nie klikaj bo atak następuje natychmiast po otwarciu strony!** Jeśli chcesz przeanalizować źródło to pobierz np. wget'em.

- https://github.com/NewEraCracker/LOIC/ - źródło i binarka LOIC

Analiza oprogramowania używanego do ataków pochodzi z badań własnych. Linki i informacje o grupie pochodzą z anonimowych źródeł. Wszelkie informacje o metodach ataków są analizą już istniejących technik. Nie wolno ich stosować w Sieci globalnej. Badania w celach edukacyjnych najlepiej wykonywać we własnej sieci lokalnej.