Laboratorium antywirusowe PandaLabs wykryło w sieci portal oferujący boty o szeregu funkcji w cenie od 95 do 225 USD. Cena całego katalogu botów to 4500 USD. Boty mają służyć do tworzenia kont na portalach społecznościowych, kradzieży tożsamości i znajomych, wysyłania wiadomości, itp. Ich twórcy twierdzą, że wszystkie boty są niewykrywalne, gdyż losowo zmieniają użytkowników, agentów i nagłówki. Zawierają także automatyczne generatory kodów CAPTCHA.

PandaLabs, laboratorium antywirusowe Panda Security, lidera zabezpieczeń działających w modelu Cloud Security, ostrzega przed siecią sprzedaży botów stworzonych z myślą o portalach społecznościowych i systemach webmail. Publicznie dostępna strona internetowa zawiera obszerny katalog programów naśladujących zachowania człowieka i przeznaczonych do użycia w serwisach społecznościowych oraz w usługach webmail, takich jak Twitter, Facebook, Hi5, MySpace, MyYearBook, YouTube, Tuenti, Friendster, Gmail czy Yahoo.

Każda pozycja wyjaśnia powód stworzenia danego bota: równoczesne zakładanie wielu kont na portalach społecznościowych, kradzież tożsamości, znajomych i kontaktów, automatyczne wysyłanie wiadomości itp. Na stronie czytamy: „Wszystkie boty działają w konwencjonalny sposób, zbierają identyfikatory/nazwy znajomych i automatycznie wysyłają zaproszenia do grona przyjaciół, wiadomości, komentarze”.

Luis Corrons, dyrektor techniczny PandaLabs, mówi: „Ciągle badamy sprawę, ale jest to kolejny przykład na to, że złośliwe oprogramowanie jest niezwykle opłacalnym biznesem dla cyberprzestępców. Katalog sprzedaży opisuje liczne zastosowania botów: niektóre mniej szkodliwe, np. tworzenie kont, inne ukierunkowane na oszustwo, w tym kradzież tożsamości, zdjęć itp.”

Najtańszy bot kosztuje 95 USD, najdroższy 225 USD. Cały katalog można kupić za 4 500 USD. Gwarantuje on niewykrywalność botów przez żadne rozwiązanie zabezpieczające, utrzymując, że mają one zdolność zmiany użytkowników, agentów i nagłówków tak często jak to konieczne, uniemożliwiając zablokowanie. Boty omijają również zabezpieczenia oparte na kodach CAPTCHA stosowane na wielu stronach internetowych, a nabywca musi tylko ustawić parametry i pozwolić botom na samodzielne działanie. Ponadto boty regularnie się aktualizują.

Niektóre z bardziej nietypowych zastosowań botów to m.in.:
Automatyczne generowanie wizyt i odtworzeń filmów w serwisie YouTube
Optymalizacja rankingów w portalu Alexa
Fałszowanie głosów w serwisie Digg
Nieograniczone wysyłanie wiadomości w portalach randkowych, takich jak DirectMatches

Boty zostały specjalnie dostosowane do każdego serwisu, a lista celów obejmuje nie tylko portale społecznościowe popularne na całym świecie, ale również lokalne strony internetowe, takie jak Tuenti, Yahoo UK itp.

„Na tym samym portalu znajduje się również oferta zarabiania na sprzedaży tych „produktów” jako przedstawiciel. To właśnie takie modele współpracy przyczyniają się do powstawania cybermafii i organizacji działających w wielu krajach. Musimy jednak pamiętać, że ten interes istnieje nie tylko dlatego, że są twórcy zagrożeń, ale także dlatego, że istnieją przestępcy gotowi za nie zapłacić. Dopóki nie będziemy w stanie uniemożliwić oszukiwania ludzi w ten sposób, ten model biznesowy będzie kwitł” - podsumowuje Luis Corrons.

Więcej informacji na www.pandalabs.com

PandaLabs