ROSNĄ KOSZTY ATAKÓW BOTÓW. 250 MLN DOLARÓW NA JEDNĄ FIRMĘ

Z danych firmy Netacea wynika, że w okresie pandemii w dużej skali wzrosła aktywność botów wykradających dane i przeprowadzających ataki na podmioty działające w sieci. W wypadku przedsiębiorstw najbardziej dotkniętych aktywnością botów ich straty finansowe sięgają 250 mln dolarów.

Działające w internecie boty to w świecie oprogramowania pewien odpowiednik robotów przeznaczonych do automatycznego wykonywania określonych operacji. Boty są coraz szerzej wykorzystywane np. w obsłudze sklepów i usług online, jednak są stosowane także przez cyberprzestępców.

Złośliwe boty to coraz większe straty

Okazuje się, że aktywność botów w nielegalnych działaniach jest na rosnącej fali. Netacea, firma zajmująca się wykrywaniem i łagodzeniem skutków ataków botów, przebadała 440 przedsiębiorstw z sektorów turystyki, rozrywki, handlu elektronicznego, usług finansowych i telekomunikacji w Stanach Zjednoczonych i Wielkiej Brytanii. Obroty analizowanych przedsiębiorstw wahały się od 350 mln do ponad 7 mld dol.

Według badania okazało się, że każdy sektor ma poważny problem z botami, przy czym dwie trzecie firm wykryło ataki na strony internetowe. 46 proc. respondentów zgłosiło, że zaatakowane zostały aplikacje mobilne, a 23 proc. (głównie w obszarze usług finansowych) stwierdziło, że boty zaatakowały ich interfejsy API.

Zautomatyzowane boty obsługiwane przez cyberprzestępców kosztują firmy średnio 3,6 proc. ich rocznych przychodów. W przypadku 25 proc. najbardziej dotkniętych podmiotów oznacza to co najmniej 250 mln dol. każdego roku.

Pandemia dodatkową okazją

Netacea zaznacza, że w czasie pandemii obecność w internecie stała się kluczowa dla przetrwania biznesu. Wprowadziła również dodatkowe wyzwania. Trudne do wykrycia złośliwe boty wyłudzają informacje od i tak już podatnych na ataki firm.

„Ubiegły rok, szczególnie trudny dla legalnie działających przedsiębiorstw, które i tak działały z bardzo niskimi marżami ze względu na spowolnienie gospodarcze, był bardzo pomyślny dla tych, którzy wykorzystują boty do wyłudzania pieniędzy z tych firm" – zaznacza w komuniakcie Andy Still, CTO w Netacea.

Różne typy botów

Netacea wyróżniła różne typy zautomatyzowanych botów:

- **Boty sprawdzające konta** pobierają nazwy użytkowników oraz hasła i testują je na stronie internetowej. Jest to również znane jako atak typu „credential stuffing" i polega na ponownym wykorzystaniu haseł.
- **Boty typu Scalper** automatyzują proces zakupu limitowanych towarów, takich jak bilety na imprezy, kończąc proces zakupu w ułamku tego czasu, jaki zająłby każdemu legalnemu użytkownikowi.
- **Boty typu scraper** służą do zbierania dużych ilości danych z witryn internetowych w celu ich wykorzystania w innym miejscu.
- **Boty snajperskie** monitorują aktywność w sieci opartą na czasie i przesyłają informacje w ostatniej chwili, pozbawiając ludzi możliwości zareagowania na to działanie na stronie.
- **Inne boty obejmują ataki DDoS**, które wykorzystują dużą liczbę botnetów do przeciążenia witryny i wyłączenia jej z sieci, boty cardingowe, które sprawdzają dane kart płatniczych czy boty służące do oszustw reklamowych.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.