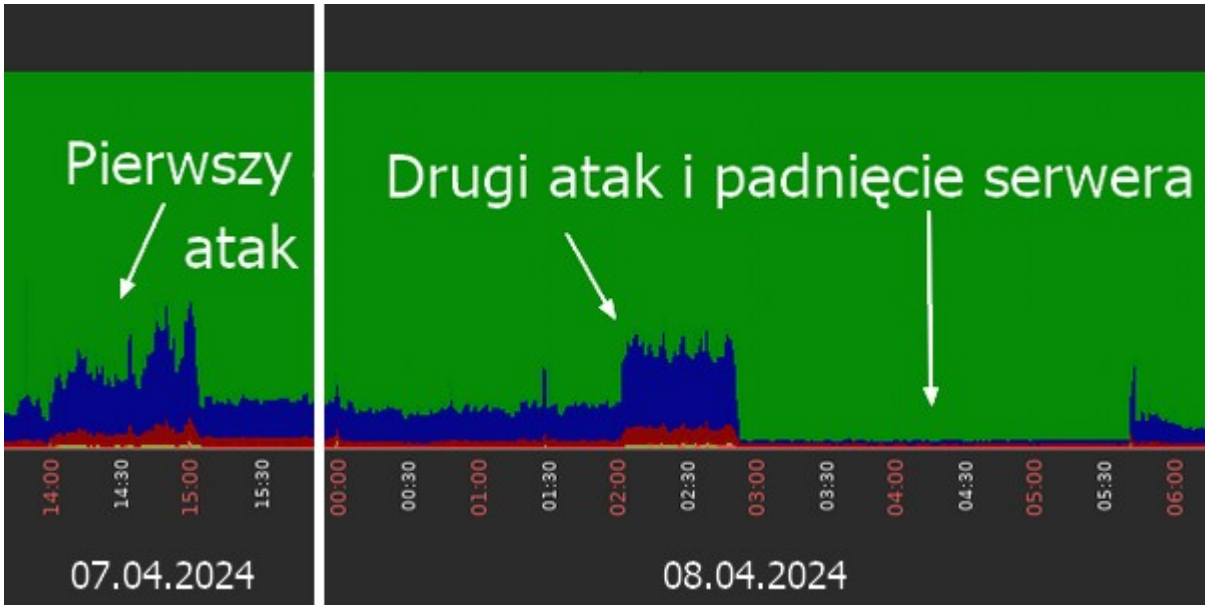
Nasz portal jest cyberatakowany!

11 kwietnia 2024

Informacja z 9 kwietnia

„Dobry wieczór. Nie mogę wejść na wolnemedia.pl. Pojawia się komunikat, jak w temacie e-maila. Czyżby atak hakerski czy może blokada ze strony władzy?” – takiego maila otrzymałem od zaniepokojonego czytelnika.

Natychmiast sprawdziłem wykresy i czy strona działa. Okazało się, że ubiegłej nocy nasz serwer był atakowany i padł na ok. 3,5 godziny. W tym czasie pojawiał się komunikat „Błąd połączenia z bazą danych”.



Według wykresów były dwa ataki. Pierwszy wczoraj, 7 kwietnia, między godziną 13:50 a 15:05, ale wówczas strona działała cały czas, aczkolwiek zapewne wolniej, a potem w nocy między godziną 2:03 a 5:42, przy czym od 2:25 do 5:40 strona była niedostępna.

Na pierwszy rzut oka wygląda to na atak botów. O ile

cyberataki z grudnia i stycznia udało się wykryć po statystykach wejść (boty atakowały z Singapuru), o tyle teraz nie widać podejrzanie wysokiej liczby wejść z jakiegoś nietypowego dla wcześniejszych statystyk państwa (drugie państwo na wykresach, po Polsce, to USA, czyli tak, jak wcześniej).

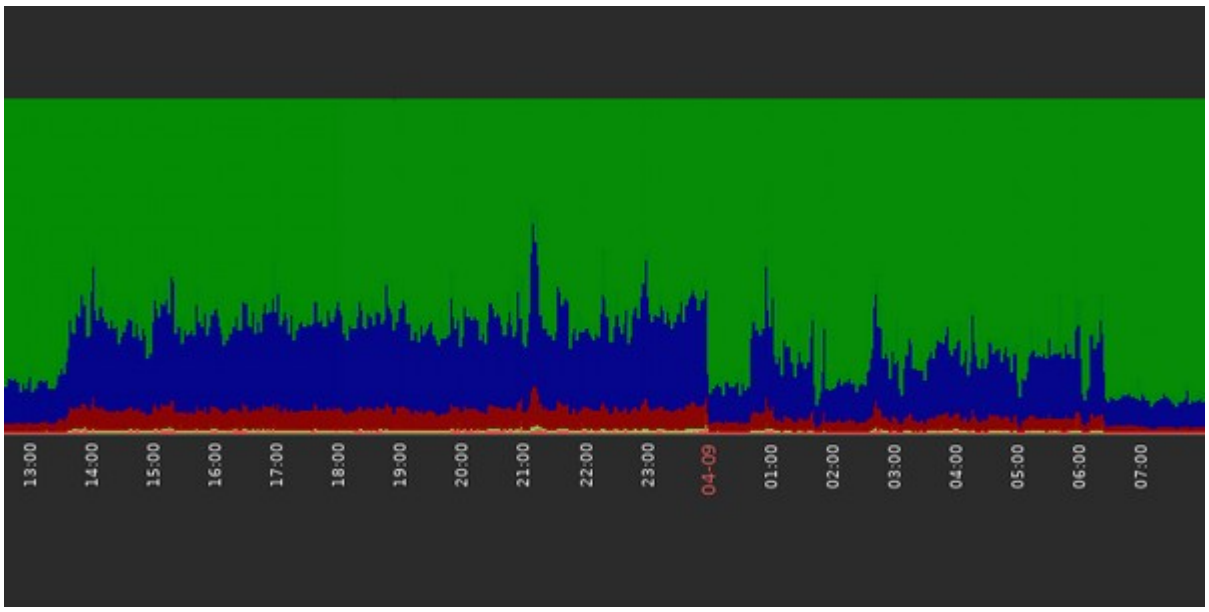
Na szczęście serwer padł wtedy, gdy większość czytelników spała, aczkolwiek sytuacja jest niepokojąca. W tym tygodniu będę częściej monitorował wykresy, by sprawdzić, czy to był jednostkowy przypadek, czy też jakiś haker obrał nas na cel. W przeszłości w podobnych sytuacjach zawsze zaczynało się od krótkich, epizodycznych przeciążeń serwera, a potem było coraz gorzej.

Dziękuję czytelnikowi, którzy powiadomił mnie o problemie z serwerem. Gdyby nie on, byłbym nieświadomy, że działo się coś złego, kiedy spałem.

Maurycy Hawranek
Administrator WolneMedia.net

Aktualizacja z 10 kwietnia

Wczoraj, 8 kwietnia, było jeszcze gorzej. Były dwa ataki, pierwszy mocniejszy od drugiego, z krótką przerwą między nimi. Sami zobaczcie wykres.



Po liczniku wejść nie widać, by boty atakujące portal nabijały licznik, tak jak boty z grudnia. Nie widać też jakiegoś wzrostu wejść z dziwnych państw. Możliwe więc, że cyberatak następuje z polskich adresów IP, bo tylko one wzrosły wczoraj.

W logach na serwerze tez nie widać niczego podejrzanego.

Kilka dni temu ukazała się nowa wersja WordPressa. Ponieważ mam ostatnio młyn na głowie (w życiu prywatnym), a aktualizacja wymaga ręcznych edycji kilku plików php (niestandardowe ustawienia dla WM poprawiające pracę wyszukiwarki), odwlekałem to do dzisiaj. I niespodzianka – po raz pierwszy od lat WordPress nie chciał się sam automatycznie zaktualizować. Zrobiłem to dzisiaj ręcznie. Nie wiem, czy to dzieło botów, które znalazły dziurę w poprzedniej wersji CMS-a i zablokowały aktualizację do nowej wersji, która być może tę dziurę załatała, aby z tej dziury korzystać, ale dzisiejszy dzień pokaże, czy jest związek.

Należy spodziewać się kolejnego cyberataku, który może objawiać się:

– bardzo długim czasem wczytywania strony;

– problemami z dodawaniem komentarzy;

– komunikatami o niedostępności strony – „Bad gateway”

– padnięciem mysql na serwerze – „Błąd połączenia z bazą danych”.

Z góry przepraszam za utrudnienia z winy cybeprzestępców atakujących „Wolne Media”.

Aktualnie szukam pomysłu, jak wytropić atak na serwerze (logi i dane statystyczne niczego podejrzanego nie wykazują) i co z tym zrobić. Jeśli ktoś z Was zna się na tym – niech napisze. Używamy wtyczek antyspamerskich i do przeciwdziałania cyberatakom. Ale wygląda na to, że boty znalazły jakąś dziurę w WordPressie.

Najlepszym rozwiązaniem byłoby przejście na inny CMS, mniej popularny jak najpopularniejszy WordPress, który jest głównym celem cyberprzestępców, ale migracja wymagałaby pomocy specjalisty, który by wszystko zmigrował i skonfigurował, aby strona zachowała podobny wygląd i funkcjonalność.

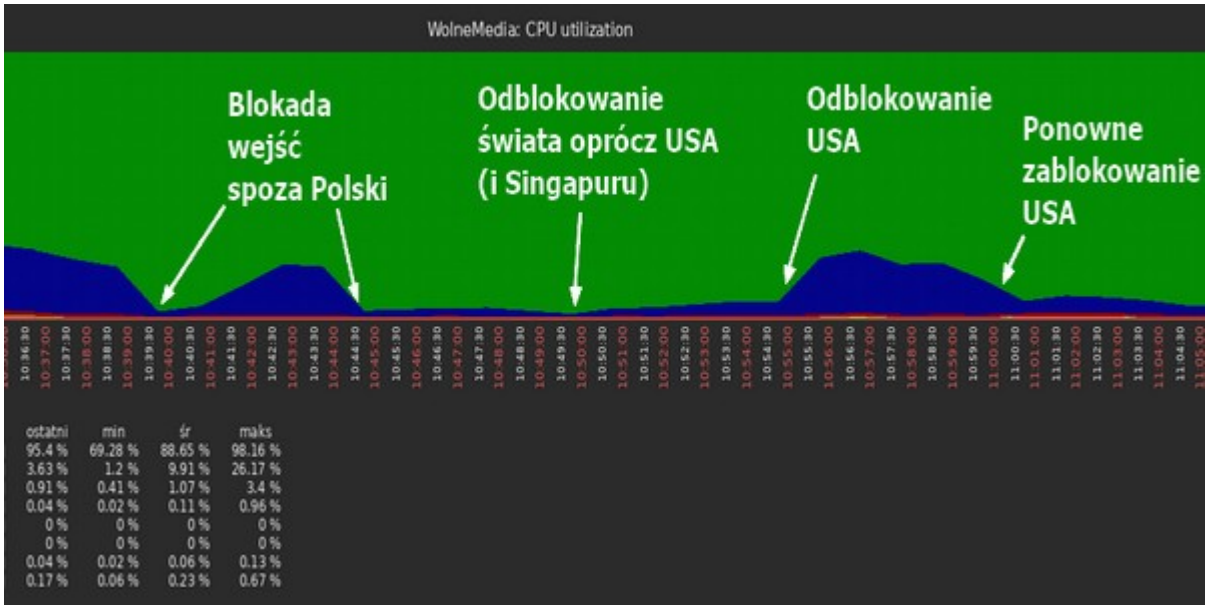
Od jakiegoś czasu trwają prace nad nakładką na WordPressa, która ogłupi boty hakerów, ale problemem jest kwestia ukończenia skryptów logowania i dodawania komentarzy w nakładce (to najtrudniejsza rzecz do napisania).

Aktualizacja z 11 kwietnia

O 8:55 zaczął się dzisiaj – 11 kwietnia – kolejny cyberatak botów. Należy spodziewać się spowolnienia strony, problemów z logowaniem lub komunikatów o problemie z wczytaniem strony. Włączyłem dodatkową ochronę, w postaci testu Captcha przy wchodzeniu na portal, ale spadek na wykresach był znikomy, więc odznaczyłem tę opcję.

Zablokowałem na chwilę wejścia spoza Polski („na oko” wg wykresów z Polski pochodzi ok. 85% ruchu, z USA ok. 15% i 10% z innych państw) i wykresy spadły prawie do zera. Następnie zablokowałem USA i odblokowałem świat. Tak to wygląda na

wykresach.



Potem użyłem opcji „also know bots” i odblokowałem USA. Wynik końcowy wyszedł podobny, ale nie wiadomo, czy narzędzie CloudFlare blokuje wszystkie boty, w tym pozyteczne roboty sieciowe indeksujące dla wyszukiwarek (np. Google). Na razie tymczasowo odblokowałem też Singapur – wykresy nie wzrosły.

Aktualizacja z 12 kwietnia

Testowałem wczoraj wtyczkę do WordPressa do walki ze złymi botami, ale mocno zamulała stronę (bardziej niż boty).

Mamy już dwa narzędzia do walki z botami. Można zablokować na czas ataków wszystkie wejścia z całego świata oprócz Polski (niestety, również te dobre, które indeksują zawartość WM dla wyszukiwarek), albo państwa, z których jest największy ruch (ostatnie ataki są z USA, ale stamtąd pochodzą też prawie wszystkie dobre boty, dlatego w statystykach nie było widać niczego podejrzanego).

Aktualny pomysł, to funkcja, by podczas włączenia blokowania wszystkich botów przepuszczane były tylko boty z Google (listę ich adresów IP można z czasem poszerzyć o dobre boty innych wyszukiwarek, z których obecnie wejścia na WM są niewielkie).

Na razie, po wczorajszych testach z blokowaniem całego świata, tylko USA i wszystkich botów, sytuacja na serwerze się uspokoiła. Jak widać na wykresie wyżej, z wczoraj, podczas blokowania całego świata, oprócz Polski, krzywa na wykresie była bardzo niska. Oznacza to, że te niebieskie obszary na wykresie, to w ok. 95% boty (dobre i złe).

W każdym razie problem został zidentyfikowany (złe boty) i ogólnie wiadomo, jak z tym walczyć (blokerem złych botów). Kwestią jest tylko brak darmowego narzędzia, bo płatne są, ale do tanich nie należą. Przydałaby się często aktualizowana online lista dobrych lub złych botów – wtedy można byłoby zrobić własny bloker (blokujący boty z listy złych, lub blokująca wszystkie boty, oprócz dobrych). Ktoś z Was zna taką? W CloudFlare w planie za 25 USD na miesiąc (240 USD na rok) mają rozszerzoną funkcję blokowania botów, a w planie za 250 USD na miesiąc (2400 USD na rok) ochrona jest bardzo silna (boty są analizowane). Nie wiadomo, ile warty jest plan za 25 USD, a plan za 250 USD to astronomiczny wydatek.