MALWARE NA STRONIE - O CO CHODZI?

Posted on 23 listopada 2015 by Maciej Cybulski

Categories: aktualności, bezpieczeństwo, dla początkujących, porady

WordPress należy do najbardziej popularnych systemów CMS, przez to jest też najczęstszym celem działań hakerów, spamerów i innych złośliwców. Czy taka sytuacja powoduje, że nie jest bezpiecznym systemem? Jest to kwestia dyskusyjna.
Możemy dbać o bezpieczeństwo wykonując aktualizacje, backupy, mając silne hasła i przestrzegając wszystkich tych ważnych zasad bezpieczeństwa, ale i tak zawsze pozostaje jakiś margines ryzyka. Nie ma 100% zabezpieczeń. Nie wystarczająco wysoki poziom bezpieczeństwa możemy próbować niwelować agresywnym monitorowaniem, backupami i wiedzą. Ale jednak zawsze jest to coś kosztem czegoś.

Obecnie dominuje opinia, że bezpieczeństwo jest procesem ciągłym, poziom bezpieczeństwa mierzony jest dwoma czynnikami: poziomem zabezpieczeń i szybkością reakcji na incydent. I chyba to najlepiej opisuje sytuację.

Każda wtyczka, która ma nas zabezpieczać, przestanie pełnić swoją bezpieczną rolę w momencie, gdy zostanie skompromitowana, gdy haker zmodyfikuje jej kod. O czym z resztą była bardzo trafna prezentacja na WordCamp Polska 2015.

Czego to dowodzi?
Z jednej strony nie ma wtyczek, które mogą nas skutecznie zabezpieczyć. Z drugiej, mimo swoich

wad, wtyczki te mogą być doskonałym narzędziem jeśli mamy wiedzę na temat ich mocnych i słabych stron oraz jakie mogą być wektory włamań.
Mając odpowiednią wiedzę i świadomość, że np. WordFence jest bezpieczna do momentu jej kompromitacji (skąd inąd stosunkowo prostej) możemy nadal korzystać z wtyczek security, ale z ograniczonym zaufaniem. Wszystko zależy od tego czy potrafimy właściwie oceniać informacje dostarczane nam przez wtyczki.

Często spotykam się ze stwierdzeniem klientów, że przecież nikt nie atakuje mojej strony, bo kto i po co miałby to robić. No i tu pojawia się skojarzenie. Czy to, że nie mamy termometru świadczy o tym, że pacjent nie ma gorączki? Do każdej wielkości fizycznej służy odpowiednie narzędzie pomiarowe. Podobnie jest z atakami DDoS i innymi. Wyposażeni w wiedzę i narzędzia możemy w łatwy sposób przekonać się, że jednak nasza strona nie jest w cale taka mało popularna i może być łakomym kąskiem dla potencjalnych intruzów.

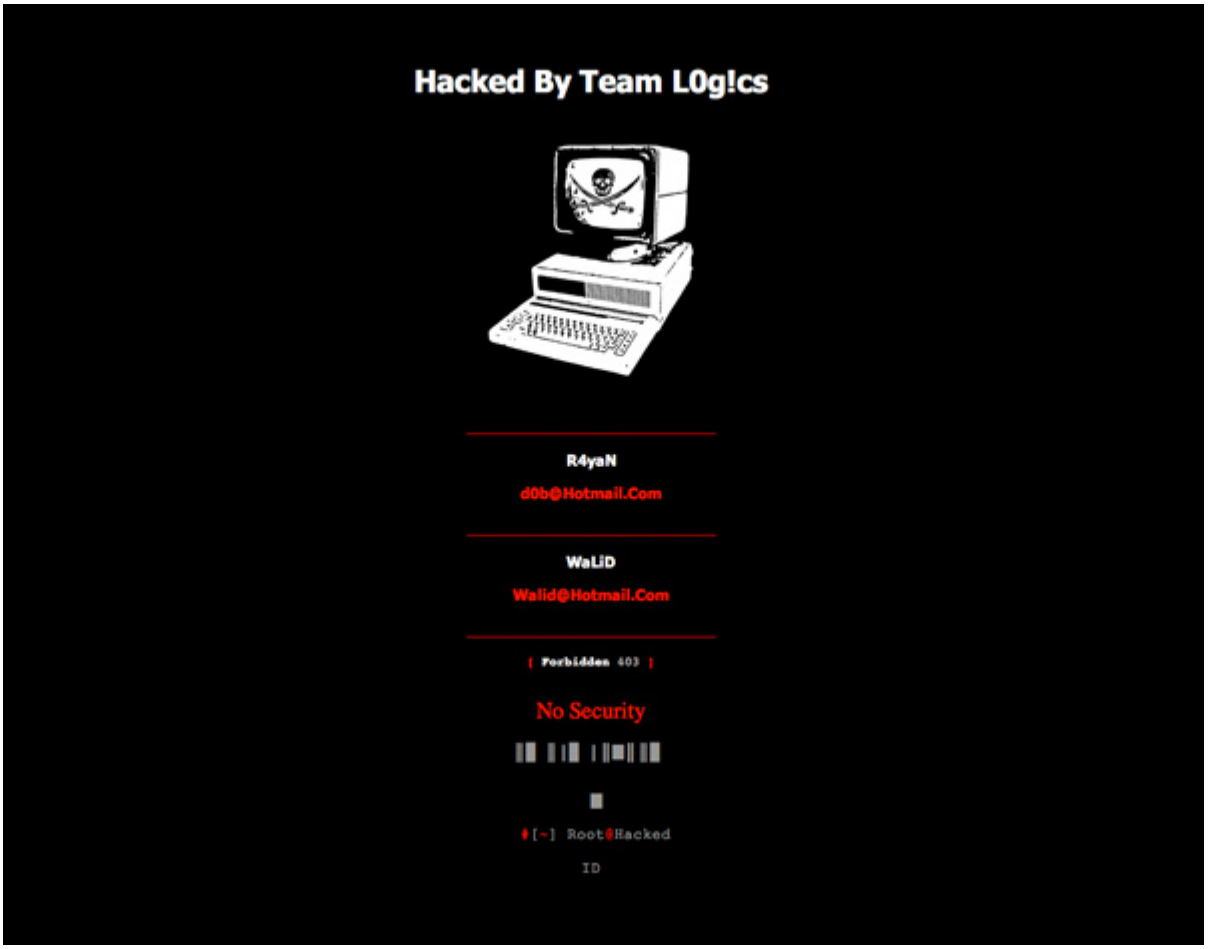
Warto zatem przyjrzeć się na jakiego rodzaju zagrożenia jesteśmy narażeni:

- **Pharma Hacks** - to te wszystkie wstrzykiwania spamu do bazy danych, lub plików na temat rewelacyjnych środków farmakologicznych itp. A dobrze spreparowany spam może być sporym zagrożeniem.
- **Backdoory** - te rozwiązania umożliwiają uzyskanie intruzowi dostępu do strony poprzez FTP lub Kokpit z uprawnieniami admina.
- **Drive by Downloads** - gdy haker używa skryptu do pobierania plików na komputer użytkownika, bez jego wiedzy, lub treść na stronie sugeruje odwiedzającemu, że plik/program, który może pobrać zawiera bardzo użyteczne dla niego funkcjonalności.
- **Wstrzyknięcia do plików i bazy danych** - dodanie do plików lub bazy danych kodu, który pozwala na właściwie dowolny dostęp do bazy, plików i ftp naszej strony
- **Złośliwe przekierowania (malicious redirects)** - to przede wszystkim przekierowania na strony ze złośliwym kodem, wirusami , trojanami itp.
- **Phising**- używany do uzyskania loginów i haseł, adresów e-mail i innych wrażliwych informacji.

No i tu dochodzimy do sedna sprawy... Nasza strona, w przeważającej ilości przypadków, nie jest tak ważna żeby właśnie ją miał ktoś atakować. Strona jest jedynie narzędziem do realizacji ważniejszych planów intruza. Jesteśmy jednym z wielu, ale tu ilość czyni siłę działania hakerów.
Używając w/w metod intruz może wykorzystać naszą stronę do atakowania innych stron lub/i komputerów, pozyskiwania danych wrażliwych podszywając się np. pod strony banków. Nasza strona jest jedynie jednym z wielu ogniw bardzo zaawansowanego łańcucha działań. Każda zainfekowana

strona/komputer może infekować następne. I tak stajemy się elementem BotNetu.

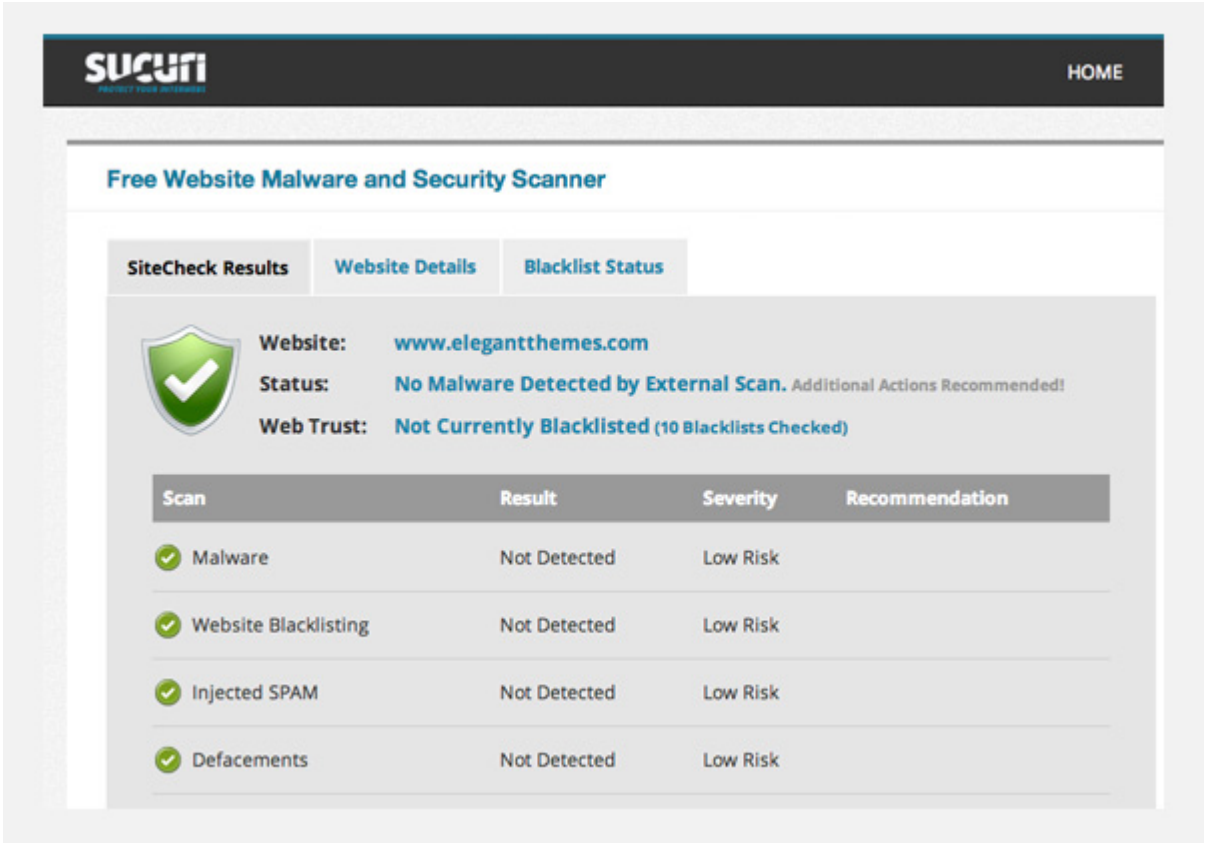
Najczęstszym sposobem myślenia, że nasza strona padła ofiarą hakerów jest myślenie, że haker uszkodził stronę i umieścił na niej wyraźną informację. Owszem tak się zdarza, ale to często po prostu próba sił i umiejętności domorosłych "hakerów", używających bezmyślnie ogólnodostępnych narzędzi analitycznych i służących do testów penetracyjnych (choćby Kali Lilnux).



Jednak w większości przypadków przeciętny użytkownik komputera nie jest w stanie zauważyć, że wszedł na stronę zainfekowaną, lub że nasza strona została zaatakowana? Dlaczego? Bo strona sama w sobie nie jest celem, jest środkiem do celu. Haker nie chce zostawiać widocznych śladów swojej obecności, bo zależy mu na tym, by móc korzystać z możliwości jakie daje mu przejęcie kontroli nad naszą stroną. W tej sytuacji złośliwy kod działa jak ukryty pasożyt.
Stąd mając swoją stronę powinniśmy być szczególnie wyczuleni na wszelkie "dziwnie" jej zachowania.

Wbrew pozorom pierwszą linią obrony powinien być... dobry program antywirusowy na naszym komputerze.
Gdy wchodzimy na zainfekowaną stronę, dobry antywirus, albo zablokuje nam do niej dostęp, albo poinformuje, że na stronie jest złośliwy kod. Gdy jest to nasza strona to już wiemy że padliśmy ofiarą ataku ;)

Jakie są zatem możliwości obrony przed takimi sytuacjami?
Mamy kilka dobrych, choć nie doskonałych, narzędzi:
Najprostszy w użyciu jest skaner Sucuri SiteCheck - skaner skanuje stronę w poszukiwaniu injekcji malware, spamu, jak również wykrywa, czy serwer na którym jest strona znajduje się na czarnej liście, co najczęściej zdarza się, gdy serwer jest używany do rozsyłania spamu. Podstawowym ograniczeniem tego rozwiązania jest to, że skaner trzeba ręcznie uruchamiać, oraz... skaner ten działa jak mocno specjalizowana przeglądarka internetowa, zatem wykrywa infekcje, które mogą się pojawić na stronie w wyniku działania np. kodu php. Monitoruje skutki nie przyczyny. Nie mniej znając lego zalety i wady, warto mieć go w swoim arsenale.



To tylko jedno narzędzie. Kolejne opiszę w następnych artykułach.

Zatem podsumowując, bezpieczeństwo strony WordPress'owej, to dość skomplikowane zagadnienie i wymaga kompleksowego podejścia na kilku poziomach. Dopiero połączenie kilku metod zabezpieczenia może dawać względnie wysoki poziom bezpieczeństwa.
O czym zatem należy pamiętać?

- Wykonujemy kopię zapasową (backup) strony w bezpiecznym miejscu - koniecznie na zewnętrznym serwerze. Kopie lokalne mają ten mankament, że jeśli haker dostanie się na serwer to nie ma pewności, że kopie nie będą zainfekowane.
- Aktualizujemy wtyczki, motywy i samego WordPress'a zawsze, gdy system nas informuje o takiej potrzebie. 98% włamań to efekt zaniechania aktualizacji, lub opóźnienia w aktualizowaniu strony. Gdy pojawia się aktualizacja np. wtyczki, pojawia się też informacja jakie błędy poprawiono. Taka informacja jest wykorzystywana również przez hakerów, np. w połączeniu z narzędziem WP-Scan potrafiącym wykryć wersje wtyczek, motywów i WordPress'a zainstalowanych na naszej stronie. A mając info o poprawkach i braku aktualizacji strony, wystarczy połączyć te fakty i wyciągnąć wnioski.

Mimo aktualizowania i wykonywania backupów, zawsze może się zdarzyć, że coś pójdzie nie tak i nie zauważymy jakiejś infekcji, choćby opisywanej już kiedyś metody "Egg drop". Dlatego ważnym jest monitorowanie stron i skanowanie skanerami malware, zarówno tymi on-line skanującymi zdalnie naszą stronę, jak też skanerami umożliwiającymi skanowanie kodu strony "od środka".

A jeśli nie mamy wiedzy i umiejętności, czy czasu, by czuwać nad bezpieczeństwem naszej strony, zawsze możemy powierzyć to specjalistom, którzy dysponują odpowiednią wiedzą i środkami by zapewnić bezpieczeństwo stronie i nam "święty spokój".

Comments

Maciej Cybulski – 2015-12-03 09:08:06
Z jednej strony masz rację, z drugiej... w wielu wypadkach wystarczy samodzielne zabezpieczenie strony, które nie jest trudne a jest w stanie zabezpieczyć nas przed sporą częścią ataków.

Maciej Cybulski – 2015-12-03 09:06:27
Dzięki za sugestię. Myślę że niebawem też i ta wtyczka zostanie przez nas opisana.

DMati – 2015-11-24 16:50:50
Widzę, że korzystasz z wtyczki Monarch, planujesz jej opisanie?

Janusz Kamiński – 2015-11-24 09:51:30
W oparciu o WordPress pracuje 25,2% stron, więc to jest bardzo zapotrzebowana informacja. Ataki stały takimi częstymi, że trzeba robić szpital wordpresowy :)