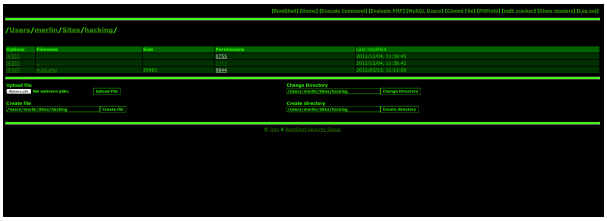


"HOUSTON, WE HAVE A PROBLEM" - CZYLI WŁAMANIE NA STRONĘ - SŁÓW KILKA...

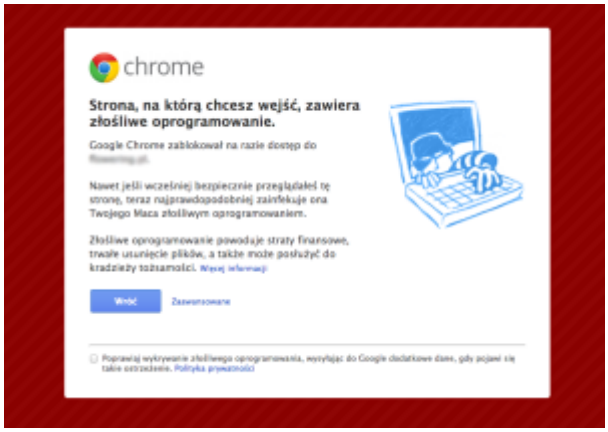
Posted on 4 grudnia 2012 by Maciej Cybulski

Categories: aktualności, inne, porady, wtyczki

Tag: antywirus, backup, bezpieczeństwo WordPressa, htaccess, IDS, ochrona przed spamem, phishing, wp-config

Pewnego wieczoru dzwoni do mnie zdenerwowany klient. Wchodząc na jego stronę pojawia się na cały ekran komunikat: "***Strona na którą chcesz wejść zawiera złośliwe oprogramowanie***"... O co chodzi? Czyżby to włamanie na stronę ? :/

Jest to przykład z jednej strony działania Googla a z drugiej robotów, bądź ludzi szukających niewłaściwie zabezpieczonych, lub nie zabezpieczonych stron internetowych.



Roboty Googla "chodząc" po stronach, analizują ich treść w celu zaindeksowania a wyszukiwarce. Natrafiając na złośliwe oprogramowanie na stronie umieszczają w katalogu właśnie taką informację. Z drugiej strony, słabo zabezpieczona strona jest podatna na włamanie na stronę i inne działania "osób trzecich" które mają na celu spam, phishing i inne tego typu działania. Po prostu złośliwe oprogramowanie uzyskuje możliwość zapisu na stronie własnego fragmentu kodu, który wykonuje już dokładnie to, do czego został napisany, a co najczęściej nie jest zgodne z zamysłem autora strony.

Przyglądając się wielokrotnie takiemu zjawisku (sam padłem kilka razy ofiarą takiego działania), zauważyłem kilka sposobów działania włamywaczy i podpinania kodu pod stronę.

1. w pliku index.php "dopisuje" się na samym końcu linijka kodu który niby wskazuje na jakiś obrazek <img> linkowany z jakiejś nieznanej strony. Okazuje się że obrazek na tamtej stronie nie istnieje a parametry jego na naszej stronie są dość podejrzane czyli np. width ="0". Zamiast obrazka na wywołuje on wykonanie złośliwego kodu.
2. Opcja już bardziej zaawansowana - włamywacz uzyskał dostęp do możliwości zapisu w jakimś katalogu na serwerze. Efektem tego jest pojawienie się w jakimś głęboko ukrytym katalogu plików zaszyfrowanych których uruchomienie pozwala włamywaczowi na praktycznie przejęcie kontroli nad serwerem. Ja na swoim serwerze znalazłem swego czasu bardzo zaawansowany skrypt i tylko przeczucie uchroniło mnie przez zainfekowaniem wszystkich stron.

Oczywiście z tym przejęciem kontroli to bardzo upraszczam sprawę, bo bardzo wiele zależy od tego jakie rozwiązania są zastosowane na serwerze i na jakim skrypcie postawiona jest strona. Z uwagi na to, że co jakiś czas migruję z moimi stronami internetowymi do różnych operatorów, jakiś czas temu miałem wątpliwą przyjemność gościć z moimi stronami w pewnej mocno reklamującej się firmie hostingowej oferującej "dobre" serwery VPS w dobrej cenie.

Po przeniesieniu stron nie wszystko od razu działało mi jak powinno więc zgłosiłem to do administratorów, a tu jeden "geniusz", pewnie żebym mu głowy nie zawracał, wpisał w menadżerze zadań cron taką oto linijkę

```
# */15 * * * * chown -Rf admin:admin /home/admin/
```

Dla niewtajemniczonych - oznacza ona że co 15 minut zmieniał uprawnienia do zapisu wszystkich plików na "admin". Na efekty nie trzeba było długo czekać. Po kilku dniach pojawiły się włamania na wielu stronach, a na tych co do których wydawało mi się że są ok (czas jednak to zweryfikował) pojawiły się przez długi czas nie zauważone jakieś niby to nie groźne pliki. Po szybkiej i dość niemiłej akcji z administratorami zmieniłem hosting. Przeniosłem domeny i strony na nowy VPS u innego operatora. Po połowie roku strony, które wydawało się, że nie zostały zainfekowane nagle zwracały "czerwony ekran" i po świadomym wejściu na stronę wszystkie jej elementy i funkcje działały niewłaściwie.

Po bardzo dogłębnej analizie okazało się że włamywacz jeszcze u poprzedniego operatora dorzucił skrypt działający jak webroot, którym później podmienił jeden z plików szablonu WordPressa, który z uwagi na to, że był komercyjnym szablonem, był też szyfrowany. Czyli na pierwszy rzut oka nie można było odróżnić czy to oryginalny plik czy podmieniony. Dopiero analiza dat i sum kontrolnych pozwoliła na zauważenie różnic. Podmieniony plik kierował internautę na stronę jakiegoś kanadyjskiego banku (tzn. stronę wyglądającą identycznie jak strona kanadyjskiego banku).

Generalnie w takiej sytuacji jedynym doraźnym rozwiązaniem jest posiadanie kopii zapasowej całości strony i odpowiednie zabezpieczenie strony po usunięciu złośliwego kodu. Dla mnie to niestety skończyło się koniecznością instalacji i konfiguracji WordPressa od początku bo archiwa które miałem również były zainfekowane.

Historia bardzo nieprzyjemna... zatem jak ograniczyć ryzyko takiego scenariusza?

1. Wykonywać własne kompletne kopie zapasowe strony.
2. Wykonywać aktualizacje skryptów strony (np. WordPressa) zawsze gdy się pojawiają.
3. Możliwie restrykcyjnie podchodzić do praw -rwx na serwerze.
4. Zainstalować Narzędzia Google dla Webmasterów, jako "system wczesnego ostrzegania" o problemach ze stroną.
5. Zainstalować wtyczki i rozwiązania antyspamowe, antywirusowe i hardeningowe. Można szukając rozwiązań, wiele godzin spędzić na szukaniu odpowiednich wtyczek, czytaniu dokumentacji, testowaniu czy dane rozwiązanie faktycznie działa w sposób dla nas użyteczny, jest stabilne i bezpieczne dla użytkownika i strony.

A można też prościej... zapisz się na nasz webinar dotyczący konfiguracji i zabezpieczenia WordPress'a, gdzie w kilka godzin przedstawimy Wam gotowe i skuteczne rozwiązanie. ... lub jeszcze prościej - **zabezpieczenie swojej strony zlecić nam.**

There are no comments yet.