

# Come ti aggiro un attacco hacker grazie a JPromoter

sabato 12 aprile 2008

Nel titolo del post scrivo attacco hacker per rendere chiaro subito di cosa andrò a parlare, ma questo termine è tutt'altro che corretto.

Dovremmo parlare piuttosto di tecniche di cracking e quindi di cracker, perché tali sono. Tentativi di forzare le barriere di sicurezza che ogni sito web dinamico deve necessariamente avere per sopravvivere in questo mondo virtuale (ma neppure troppo) bazzigato sempre più spesso da figli di puttana che non hanno, evidentemente, nulla di meglio da fare.

Oltre una settimana di pura sofferenza per capire come arginare "questi signori" che hanno preso di mira il mio dominio e che mi hanno causato piccoli problemi alla mia home page con attacchi ripetuti in vari orari e per diverse volte ogni giorno.

Poi, ieri sera prima di addormentarmi, l'illuminazione. Un rimedio semplice e vecchio come il mondo per metterglielo in culo. Spero solo possa funzionare.

Analisi dell'attacco.

La tecnica è quella di passare attraverso la barra degli indirizzi una stringa "maligna" nella speranza di trovare una falla di sicurezza che permetta di ottenere un accesso a livello admin (amministratore) sul dominio preso di mira. Questo detto in soldoni. Non è il caso di entrare in tecnicismi.

Inutile dire che la mia installazione di Joomla è perfettamente aggiornata, così come tutti i componenti aggiuntivi. E' fondamentale mantenere tutto aggiornato per limitare al minimo i possibili danni dovuti ad un attacco. Provate a pensare cosa può fare un cracker che riesce ad ottenere l'accesso come amministratore sul vostro dominio. Diventa lui padrone, con diritti di vita e di morte su tutto ciò che avete pubblicato. Potrebbe tranquillamente estromettervi dal vostro stesso dominio se solo volesse.

Nel mio caso non è successo nulla di simile. Di fatto non sono riusciti a fare alcun danno. La parziale compromissione della mia home page è dovuta ad un effetto collaterale dell'attacco che ha interagito in modo imprevedibile con un componente SEO (JPromoter) che uso per riscrivere le Url del mio sito.

Nella pratica JPromoter interpretava la stringa di attacco e, nel tentativo di riscriverla per renderla più "leggibile", gli assegnava come Url <http://davide.pedrelli.eu/> e cioè la home del mio sito. La conseguenza di questa riscrittura anomala porta ad una catena di errori in bella vista per nulla piacevoli.

Temporaneamente tamponare la ferita per evitare l'emorragia.

La prima volta che ho visto la home in quelle condizioni sono sbiancato. Ho immediatamente capito dagli errori stessi che il problema era in JPromoter, dove ho trovato una strana Url riscritta e assegnata alla home. La cancello e tutto torna a funzionare perfettamente. Anche il mio cuore riprende a battere con regolarità.

Se non ché, gli stronzi tornano all'attacco e io mi ritrovo a dover cancellare a mano e più volte al giorno le stringhe di attacco. E' una situazione insostenibile. Non posso andare avanti così. Devo trovare una soluzione.

Possibili soluzioni.

- Rimuovere JPromoter?

Ma questo comporta dover trovare un altro componente SEO e riscrivere tutte le Url per renderle uguali a quelle attuali, pena la perdita dell'indicizzazione sui motori di ricerca con le conseguenze che vi lascio immaginare. Per non calcolare il tempo necessario.

No. Questa sarà l'ultima spiaggia. Per ora non se ne parla neppure.

- Cambiare il template?

Da alcune prove che ho effettuato su un sottodominio di test iniettando io stesso la stringa maligna, ho notato che il template ha la sua importanza. Se cambio template risolvo il problema.

Ma questo template mi piace. Ci ho lavorato come un mulo per renderlo così. Devo ricominciare da capo? Non è accettabile. Deve pur esserci una terza via. Pensa Davide. Pensa.

La terza via.

Un fulmine a ciel sereno. Ecco la possibile soluzione. Semplice ed efficace. Che salva capra e cavoli. Riscrittura della home page + redirect forzato. Può funzionare ed è facile e veloce da implementare.

Come mia abitudine, uso ciò che ho a disposizione + un pizzico di fantasia.

Ho sfruttato quindi la capacità di riscrittura delle Url di JPromoter volgendo a mio vantaggio e riscrivendo la home page da <http://davide.pedrelli.eu/> a <http://davide.pedrelli.eu/prima-pagina.html>.

Questo a livello di navigabilità interna del sito ha tecnicamente risolto il problema.

Rimane comunque scoperto il secondo aspetto e cioè quello di chi arriva sul sito attraverso link diretto (<http://davide.pedrelli.eu/>). In questo caso infatti la riscrittura della home non ha alcun effetto.

Qui ci vuole un pizzico di fantasia.

Creo quindi una pagina web che chiamo index.html (la classica home page di un sito HTML puro) e la piazco nella root di <http://davide.pedrelli.eu>

Lo scopo è quello di sfruttare una caratteristica dei web server, i quali offrono automaticamente ai browser questa pagina (index.html, ove presente) nel caso non ci sia una specifica e diversa richiesta da parte loro.

Per completare il tutto, nella pagina index.html vado ad inserire il codice per un bel redirect che forza il browser a spostarsi su <http://davide.pedrelli.eu/prima-pagina.html> e il gioco è fatto.

L'accesso diretto alla vera home page è garantito dal redirect presente in index.html e la navigabilità interna del sito dalla riscrittura delle Url da parte di JPromoter.

E... in culo a 'sti stronzi che non hanno un cazzo da fare!

{mosloadposition correlati}