HTML/Crypted.gen attacca WordPress e Joomla

di Paolo Franzese

Interessante spiegazione dell'attacco a imaginepaolo presa da http://www.settorezero.com/:

> Sta accadendo sempre più spesso ultimamente, che molti siti basati su WordPress e Joomla, vengono attaccati in qualche modo dal **Trojan** segnalato da Avira come " **HTML/Crypted.gen**". Non sono riuscito a capire se si tratta di un problema relativo a bug esistenti in questi due sistemi di publishing (ma ne dubito) o piuttosto da un virus **che ha attaccato i server** che ospitano tali siti.
>
> Quest'ultima ipotesi mi è stata avvalorata dal fatto che tutte le persone che ho contattato e che hanno avuto lo stesso problema, hanno tutti l'hosting presso lo stesso provider. Non muovo ancora accuse per ora perchè la cosa è alquanto anomala e in rete non ho trovato informazioni soddisfacenti per poter fare un'ipotesi valida, per cui le mie sono soltanto supposizioni e vanno prese come tali.
>
> Nel frattempo spero che questo post possa essere d'aiuto e oggetto di discussione per capire da dove si origina il problema.
>
> C'è innanzitutto da dire che il virus altera le pagine (ma non sempre tutte le pagine del sito) con estensioni html, php, asp e js, aggiungendovi un **codice javascript criptato**, che *più o meno* inizia in questo modo:

```
<script language="javascript">$a=\
"Z64dZ3dZ22q|se|qdu]qwys^e}rub8tqiZ3c0}
```

> Dico "più o meno" perchè non a tutti si presenta allo stesso modo, è facile comunque identificare il codice maligno perchè, come si vede, è in qualche modo offuscato: non si leggono parole chiave ma soltanto sequenze di caratteri *apparentemente* assurde.
>
> Relativamente a wordpress, invece, il codice malevolo viene generalmente inserito in tutte le pagine "index.php" e inizia in questo modo:

```
1 <?php ob_start("security_update"); function security_update($buffer){ret
  Z64dZ3dZ22q|se|qdu]qwys^e}
```

> *Pare* che lo script non crei danni e venga rilevato solo da Avira (chiedo conferme). Il problema si risolve eliminando lo script ritenuto dannoso dalle pagine, oppure

ricaricando una copia sana delle pagine sul server.

Alcuni utenti, invece, dopo aver preso un virus, si ritrovano la copia del sito (o altre pagine web) salvate sul proprio pc con tale problema: quindi l'attacco pare che sia "locale" e non remoto: le pagine sembrano essere attaccate sullo stesso pc in cui risiedono. Questo mi fa pensare sempre più che sia un problema di hosting: difatti in tantissimi hanno sul proprio pc una copia del sito non infetta, mentre sul server è invece presente questo script nelle pagine.

La soluzione per potersi tenere al riparo è avere sempre un backup aggiornato del proprio sito sul PC e ordinare il backup del sito web qualora non ne fossimo provvisti.

Riporto qui alcuni link utili (per lo più riguardanti wordpress) relativi al problema esposto:

http://codex.wordpress.org/FAQ_My_site_was_hacked

http://www.wordpress-it.it/forum/topic/12452

WordPress 2.8.5 ; Oltre 100 attacchi Hacker su Aruba

Da un articolo scritto da Paolo Franzese il 25 Settembre 2017