JHacker Watch system plug-in
Trial Edition

****

A website monitoring plug-in for Joomla! 3
****

IMPORTANT NOTE ABOUT GENUINE SOFTWARE FROM INNATO

This software is only guaranteed being genuine and original if obtained/downloaded directly from Innato BV (www.innato.nl).
Any other source may (either unintentionally or willingly) provide you with software that has been modified to perform different, incomplete or additional tasks that you may not be aware of. Innato BV can never be held responsible, nor will be liable for any consequences that the use such software may have.

Please post bugs on our forum on http://www.innato.nl/forum.html or email us on webdesign@innato.nl

INTRODUCTORY REMARKS

In this documentation, the working of and the technology behind this plug-in is not explained in too much detail. The reason is that we do not want to educate those who enjoy the defacing and mutilation of other people's websites.

ABOUT THE TRIAL EDITION

This Trial Edition is a very basic and limited freeware version of the Standard Edition, only meant to give you a taste of the 'real thing'. The Standard Edition offers a better and extended protection at a VERY AFFORDABLE PRICE; it has more functions and configuration options. The Business Edition is the professional solution for business websites.
The additional options that are available in the Standard Edition and the Business Edition are summarised at the end of this document.

WHAT THIS PLUG-IN DOES

This plug-in continuously monitors your Joomla! install in a way that it checks whether critical user account details have been changed or files have either been modified or added and that are not part of a standard Joomla! install. It therefore provides an additional protection against website hacking attempts. The plug-in also slows down repeated back-end log-in attempts to make brute force attacks frustratingly ineffective (for the potential hacker that is).
The plug-in does NOT prevent hacking attempts and cannot guarantee that your website will never be hacked, but it counteracts certain unusual activities and - most importantly - notifies the site administrator(s) of these activities, thus making a hack attempt less successful and providing the information for an additional line of defence.

WHEN IS THE PLUG-IN FIRED?

The JHacker Watch plug-in is fired upon every visit to both the website's front- and back-end. If your website has a great number of registered users, its frequent firing may impact the performance of your website as perceived by your website visitors. The **Standard** and **Business** editions include the option to set an interval for front-end calls.

REQUIREMENTS

- Joomla! 3.1 or later
- PHP 5.3 or higher, PHP 7, PHP 8

DISCLAIMER

This software is provided ‘as is’, without any promise or guarantee that it will perform to your expectation(s). The software has been carefully developed and tested in a standard Joomla! core software environment and has been approved for use. There may however still be flaws, bugs and omissions in the software. We will try to fix these, but can never be made responsible or liable for the consequences of using the software.

Basic install and setup instructions for JHacker Watch plug-in for Joomla! 3.x – TRIAL EDITION

This information is to be considered a basic guideline and is provided as is, without warranty.
Your Joomla! installation and setup may be different from the basis for these instructions.

HOW TO CHECK FOR UPDATES

- Open the JHacker Watch plug-in manager screen via 'Extensions' / 'Plugin Manager'.
- Under "Description" in the panel at the left near the plug-in logo, you will find the current version and a link to check for updates.

INSTALLATION AND UPGRADE

Install or upgrade via Joomla! back-end. Your settings will not be lost.

HOW TO DEAL WITH NOTIFICATIONS/ALERTS ISSUED BY THE PLUG-IN

If the plug-in has issued a notification or alert (system message), this notification/alert will describe the detected event only in broad terms. This is intentional, in order to keep information about the exact nature and origin of the event away from potential hackers. To see more detail, you can configure to have an email notification sent to you (see Advanced Options). The email notification will contain more specific details about the event.

If you have resolved the issue(s) that raised the notification or if you want to reset the plug-in because the event was legitimate, you can RESET the Account Monitor and/or the Directory Monitor as described under the Advanced Options section. The notification/alert will then be cleared.

SETUP / OPTIONS

WARNING:
If the root directory of your website already contains files additional to a standard Joomla! install, you are advised to make a backup of these root files before configuring and enabling this plug-in.

You should enable the plug-in immediately after installation. This is completely safe, because the plug-in default settings are such, that no special actions will be taken yet. Only repeated back-end log-ins will from now on become slower upon every failed attempt, this is the intended behaviour.

IMPORTANT NOTES:

- Since the default install settings are not taking any special actions, your website will not yet be monitored after the install. Therefore, you are strongly advised to review all plug-in options; see the option descriptions for recommended settings.

- After reviewing and setting the plug-in options, you should make a backup of the plug-in SQL data table. The table is named "_plg_jhackerwatch_prg_data".

PLUGIN OPTIONS

BASIC OPTIONS

AUTO-REMOVE ROOT FILES

The auto-remove function affects Joomla! root files only, i.e. it does not affect any (sub) directories and their content.
When the plug-in detects a root file that is not part of a standard Joomla! install, you can have it automatically removed. By default, this option is disabled.
In the Trial edition, only two options are available. The Standard and Business editions have more autoremove options.

'Only non-standard index files' automatically removes only root files that have the name format 'index.xyz', where xyz is any file extension (may be more than three characters). The standard Joomla! file index.php is excluded from removal.

NOTES:
If a system warning message is shown that the auto-remove function failed to delete files, please check the read/write permissions of the parent directory of the website install, then set/chmod these permissions to 757 (only the parent directory, i.e. not recursively) and refresh the back-end admin page. If the warning has disappeared, the auto-remove function is working properly.
The above may happen, for example, if you have installed your website in a sub domain of your master domain. For example, you own the domain 'mydomain.com' and you have installed Joomla! in the sub domain 'tester.mydomain.com'. Your server may have been configured in such way, that the sub domain website install is placed in a sub directory of the master domain, e.g. in '/public_html/tester', and that the default read/write permissions of this sub directory are too strict for the auto-remove function of the plug-in.

ACCOUNT MONITOR OPTIONS

ACCOUNT MONITOR

If enabled, selected account details will me monitored, meaning that any changes in these details will be detected and generate a notification. Setting all options under 'scope' to 'no' (see below) will disable the account monitor. Only changes in the account details will be monitored, in other words: the account details content are not read.

SCOPE

Select the user details that are to be monitored. Please be aware that users may change their password and email address, therefore including these in your selection may lead to an increased number of detections and notifications.

ACCOUNT MONITOR RESET

This option rebuilds the plug-in account monitor data and brings these in line with the current account states. Resetting the account monitor will not affect the Joomla! accounts database.

Example:
A user has changed the email address. If the email address option was included in the account monitor scope, a notification will be raised. If the email change is legitimate, you can reset the account monitor to validate the change. No new notification will be raised, unless this (or another) user changes the email address again.

Recommendation:
If you are done with testing the various plug-in options and settings and have established a 'final' configuration, you should reset the account monitor in order to refresh and sanitise the plug-in database.

DIRECTORY MONITOR OPTIONS

DIRECTORY MONITOR

Enable or disable the directory monitor here.
The directory monitor regularly scans the directories in the root plus selected sub directories (see also the 'preset' option below). If directories have been added/removed or directory names have changed, a notification will be generated. In addition, the files inside the directories will be included in the scan. If files have been added/removed or file names have changed, a notification will be raised.
Which directories will be monitored, depends on the selected 'preset' option, see below.

PRESET DIRECTORIES

This option defines which (sub) directories are monitored.

'Basic' All root directory names (not root dates) are monitored, including non-Joomla! and including the JHacker Watch plug-in itself. No other files inside directories and no sub directories. Root files are taken care of by the 'Auto-remove root files' configuration.

'Critical' All root directory names (not root dates), including non-Joomla!, and some critical sub directories are monitored. The first level directories and files inside the root directories and critical sub directories are included in the scan. Root files are taken care of by the 'Auto-remove root files' configuration.

'Standard' All root directory names (not root dates), including non-Joomla!, and all standard Joomla! sub directories are monitored. The first level directories and files inside the root directories and sub directories are included in the scan. Root files are taken care of by the 'Auto-remove root files' configuration.

See also under 'Exclude Directories' below.

EXCLUDE DIRECTORIES

Enter (sub) directories that must be excluded from being monitored. Give the full (sub) directory path relative to the root, e.g. /mydir/mysubdir. It is permitted to exclude (sub) directories that have been included by the monitor preset value; you may even exclude root directories. Separate entries by a new line or comma.

Recommendation:
The 'standard' preset (see above) includes directories of which the content may change regularly due to admin or website activity, for example '/media'. You may also have installed extensions that have created a root directory of which the content varies. Therefore, it may be wise to exclude specific (sub) directories from the monitor, in order to prevent frequent notifications.

DIRECTORY MONITOR RESET

This option rebuilds the plug-in directory monitor data and brings these in line with the current state.
Resetting the directory monitor will not affect the Joomla! directory structure.

Example:
You have installed a new component. There were no notifications before, but the install has created a new directory in the /components folder and therefore, a notification will be raised. To validate the change and to add the new folder to the directory monitor (provided the monitor preset is set to 'critical' or higher), you can reset the directory monitor.

Recommendation:
If you are done with testing the various plug-in options and settings and have established a 'final' configuration, you should reset the directory monitor in order to refresh and sanitise the plug-in database.

NOTIFICATION OPTIONS

ENABLE EMAIL LIST
Enables sending notifications to configured email addresses, see below.

NOTIFICATION EMAIL LIST
Here you can enter email addresses, that will receive plug-in notifications.

RESEND ALL NOTIFICATIONS
Select 'Resend' to have all email notifications sent once more to all configured recipients. The notifications will not only be sent again, but the information will also be updated to the current website status.
To avoid email flooding of recipient email accounts, notifications are sent only once for each notification type. So, for example, if the first user account has been added, you will be notified of this event, but you will not be notified of the second user account that has been added shortly after the first event. By resending all notifications, you will be sent an overview of all added user accounts so far.

Recommendation:
If you have received various notifications and are ready to resolve all reported issues, delete all JHacker Watch plug-in notifications from your email and select the 'Resend' option.

ADVANCED OPTIONS

DATA TABLE RESET
You should never need to use this option. This option is only to be used when the plug-in data table has become corrupted or compromised by a hacking attempt and you have no website backup or other means for data recovery available. Can only be executed by Super Administrators.
This option completely rebuilds the plug-in data table based on the CURRENT user account, directory and file data of the website. So, if user accounts, directories or files have been tampered with, all these corrupted data will become part of the new plug-in data table and will be considered as a genuine part of your website. Therefore, use this option with extreme caution and only as a last resort if anything else failed.
To execute the data table reset, you must enter the two words "RESET TABLE" in the option field; these words must be in capitals.
Again: By executing this option, you will be approving that malicious and corrupted data that possibly exist will be considered by the plug-in as a genuine and legitimate part of your website!

Recommendation:
Before using this option, you should first consider the following:

- Are you sure that all user accounts, website directories and files are 'clean' - in other words only the plug-in data table has become corrupted? If so, you can safely reset the plug-in data table.
- Can you reinstall a recent and 'clean' backup of only the plug-in data table? If so, reinstall it. The table is named "_plg_jhackerwatch_prg_data". Next, resend all notifications, check your email and see what issues have been reported; then correct these.
- If you are in the position to access and check user accounts, website directories and files, you can repair all these and then reset the plug-in data table under 'Advanced Options' in the back-end plug-in manager. Please note that a file's content may have been changed without changing the file name; such hack will be more difficult to trace.
- The best route to repair is always to reinstall a 'clean' and recent full backup of of your website (all tables and all files).

REMOTE MONITORING KEY

Remote Monitoring is a powerful additional warning service. This option requires a personal key, that can be obtained by clicking the link below the option title. A subscription fee applies.

Why use remote monitoring?

A malicious hacker who obtains full access to the administrator back-end of your website, will be able to unpublish (disable) the JHacker Watch plug-in all together. If the hacker is smart enough, this is the first thing he or she will do before anything else, thus making sure that further changes to the website remain unnoticed by the plug-in. With Remote Monitoring enabled, such event will however NOT go unnoticed.

How it works

When the plug-in Remote Monitoring option is enabled, by entering and saving the personal key that you have obtained, a short encrypted character string will be added to your website's pages. This string will not appear anywhere in the viewable content of the website, but can be read by our remote monitoring software, residing on our servers. The character string contains only little data about the website where the JHacker Watch plug-in has been installed and about the plug-in itself: the website domain, the IP address and the plug-in type. No information about the content or setup of the website and its files and database(s) is included whatsoever.

After you have registered a personal Remote Monitoring key and completed the procedure, your website will be regularly visited by our remote monitoring server, to see if the JHacker Watch character string is still there and is still containing the same data (domain, IP and plug-in type) as we have on record from your registration. If not, you will be notified!

So - for example - if a malicious hacker were to disable the plug-in all together, the character string will be missing from your website pages and our monitoring software will notice this and notify you by email.

BROWSER MODE

Our remote monitoring software that will visit your website regularly (when enabled), is a so-called 'web bot' that will identify itself as 'JHW Bot', 'JHWBot' or 'jhwbot'.

If you (or your ISP) have disabled or blocked access by web bots, you can still use the Remote Monitoring option by setting the 'Browser mode' option to 'yes'. Our remote monitoring software will then access your website as a regular internet visitor using a Firefox browser. If you are keeping track of your visitor statistics, you will see it coming from The Netherlands (.nl) with our IP address (currently 89.18.176.122).

DISABLE IP MONITOR

As explained above, our remote monitoring software will regularly evaluate the IP address of your website against our record from your Remote Monitoring registration.

If you or your ISP are using a dynamic IP regime, whereby the IP address of your website changes more or less frequently, you will be receiving regular email notifications stating that there is an IP problem with your website.

To avoid these notifications, you can exclude the IP address from being monitored, by setting the 'Disabe IP monitor' option to 'yes'.

Please note: If you set this option to 'yes', all changes to the IP address of your website, i.e. both intentional and unintentional, will no longer be detected by our remote monitoring software. Therefore, we recommend that you leave this option to its default setting ('no') at the start, and only change it if you are sure that your website is indeed subject to dynamic IP addressing.

ABOUT COOKIES

The JHacker Watch Trial Edition does not use cookies.

18-Feb-2022
Innato BV
www.innato.nl

The following pages describe the additional functionalities and options of the Standard Edition and the Business Edition.

The Standard Edition is an extended version of the plug-in. It is well suited for most professional websites and has the following additional options.

ADDITIONAL OPTIONS STANDARD EDITION

BASIC OPTIONS

FRONT-END CHECK FREQUENCY
Plug-in activation interval. Can be set to 5 minutes or 'each website call'.

AUTO-REMOVE ROOT FILES
Additional option **'All non-standard files'** automatically removes all non-standard Joomla! root files.

EXCLUDE ROOT FILES FROM REMOVAL
Files to be excluded from automatic removal by the plug-in.

ACCOUNT MONITOR

SCOPE: Added option to monitor User Groups.

MONITOR ADDED ACCOUNTS
Monitors the creation of additional user accounts.

MONITOR REMOVED ACCOUNTS
Monitors the removal of user accounts.

DIRECTORY MONITOR

TIMESTAMP MONITOR
Monitors the timestamps of directories and their first level files.

FILE SIZE MONITOR
Monitors the file sizes of first level files inside monitored directories.

PRESET DIRECTORIES: 'Extended' option added

INCLUDE DIRECTORIES
Directories that must be included in the monitor, in addition to the preset. The first level directories and first level files inside the included directories will be monitored.

EXCLUDE ROOT FILES
Exclusion of individual root files from file date/size monitoring. Root files only.

The Business Edition is the most complete version of the plug-in. It is well suited for professional websites. It includes a full business license and the following additional options vs the Standard Edition.

ADDITIONAL OPTIONS BUSINESS EDITION

BASIC OPTIONS

FRONT-END CHECK FREQUENCY

Additional options to select from

ALLOWED ADMIN IP

Configures administrator back-end access from specified IP addresses only.

TIMESTAMP MONITOR

Additional option to allow for a minor difference between recorded and current timestamps. This may prevent frequent plug-in notices for hosting servers that do not keep their clock accurately synchronised.

ACCOUNT MONITOR OPTIONS

DUPLICATE ACCOUNT DATA

By default, Joomla! requires a unique username and email address for each user account. If this option is enabled, the plug-in will check for multiple occurrences of the account items set in the 'account monitor scope' option, EXCEPT user groups.

DIRECTORY MONITOR OPTIONS

EXCLUDE INDIVIDUAL FILES

The Business Edition allows the file date/size monitoring exclusion for individual files in a (sub) directory, in additon to root files only.

ADVANCED OPTIONS

NOTIFICATION GROUP

Administrators and/or Super Users can be notified as a group.