Background Process Killer

(WHM >> Home >> System Health >> Background Process Killer)

Overview
Set up the process killer
Processes that this feature can kill

Overview

This interface allows you to select processes that the system will terminate when the `upcp` script calls the system maintenance script (`/scripts/maintenance`) every night. After the system terminates a process, it will send you a notification via email.

Note:

The background process killer does **not** terminate processes that run from the `/usr/bin` directory because the system assumes that the system administrator intentionally installed programs into that directory (for example, the system administrator installed `BitchX` via RPM).

Set up the process killer

1. Select the checkbox that corresponds to the processes that you wish to automatically terminate.

   Note:

   We recommend that you select **all** of the available processes.

2. If you wish to allow specific users to run any of the processes that you have selected, enter their names in the *Trusted users* text box.
   - For example, if you add `username` to the list, the user `username` can run the processes that you select.
   - You do not need to add users with a UID below 99.
3. Click *Save*.

Processes that this feature can kill

The processes in the following list often result in denial of service attacks (DoS or DDoS) that launch from or against your server.

Note:

Malicious users often rename the process so that it is difficult to find. However, this WHM feature detects the process no matter what name it uses, and it automatically shuts the program down.

Process	Description
`BitchX`	This is a popular command line IRC (Internet Relay Chat) client.
`bnc`	This is a common IRC bouncer. Bouncers allow users to hide the source of their connection and route traffic through secondary locations. Hackers often use these in denial of service attacks.
`eggdrop`	This is a popular IRC bot. A bot is an automated system that will execute a set of commands. In this case, the bot executes sets of IRC co mmands to moderate IRC channels (chat rooms). However, attackers can use this program to create botnets for denial of service attacks.
`generic-sniffers`	Third parties use sniffers to collect and analyze packets of information as they transmit between computers. Often, hackers use sniffers to analyze the data for encryption methods and gain access to networks to which they should not have access.
`guardservices`	This is an IRC bot. For more information, see the definition of `eggdrop` above.
`ircd`	This is the daemon that enables IRC. IRC is an attractive target for malicious users, because the server typically runs for a long period of time. This allows hackers to use packet sniffers to extract information and launch attacks.
`psyBNC`	This is a popular IRC network bouncer. For more information, see the definition for `bnc` above for more information.
`ptlink`	This is an IRC server. For more information, see the definition of `ircd` above.
`services`	This is an IRC bot. For more information, see the definition of `eggdrop` above.

Additional documentation

- Installation Guide - Customize Your Installation
- WHM Scripts
- The onboot_handler Script
- The cpanel.config File
- System Administrators FAQ