pl.backdoor.connectback.001 - Sucuri Labs

Published: 2019-04-02 · Archived: 2026-04-05 13:38:14 UTC

Backdoors are server-side malicious scripts which are intended to perpetrate malicious acccess to the server. The typical example of such backdoors are various File Managers, Web Shells, tools for bypassing admin login or various one-purpose scripts allowing the attacker to upload and run another type of malicious scripts. The payload is PHP based, thus intended for server-side use and the payload is executed directly on the server, while the site is loaded. Only the payload result (such as Web Shell environment) is visible in the browser, not the malicious code itself. It's very common, that backdoors don't have any visible signs in the site code and it's impossible to detect them by accessing the infected site from outside. Server level analysis is necessary in case of infection by this type of malware.
This malware when executed connect back to the attacker server and accept arbitrary commands, permitting the attacker to have full control of the server.

Affecting

Any vulnerable website with perl support. Outdated software or compromised passwords can act as an infection vector.

Cleanup

Inspect your server looking for any unknown perl file and remove them. Also, you can sign up with us and let our team remove the malware for you.

Dump

```
#!/usr/bin/perl
use Socket;
print "Data Cha0s Connect Back Backdoornn";
if (!$ARGV[0]) {
printf "Usage: $0 [Host] <Port>n";
exit(1);
}
```
