Malware stole my FTP credentials!

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- CuteFTP, CuteFTP Home, CuteFTP Pro versions 7 and 8

SYMPTOM

Malware stole my FTP credentials!

RESOLUTION

The problem with being one of the world's best FTP clients is that bad people try to hack you. Certain malware attacks look specifically for files used by CuteFTP, then attempt to use the information in the file to access the FTP sites that you have configured in your Site Manager.

First of all, understand that, unlike certain other FTP clients, CuteFTP's Site Manager data is NOT stored in plain text. In addition, CuteFTP Pro and Home versions include optional encryption to protect your Site Manager data. Protecting your Site Manager data is as simple as configuring a Site Manager "master" password. This master password is different than the individual passwords that you use to connect to your FTP sites. The Site Manager password secures all of the Sites in your Site Manager using encryption, locking down the Site Manager data file so that even CuteFTP can't read it until you enter the password. (Note that if you forget the password, you will not be able to use the protected Site Manager data and will have to create new Sites.)

To configure the Site Manager password, click **Tools > Site Manager > Security > Encrypt Site Manager data**, then provide a secure password in the dialog box that appears. To be secure, a password should contain at least 8 characters, both numbers and letters, upper and lower case, with punctuation. For example, !Ts6J4?5 is more secure than IamSecure.

In addition to securing your Site Manager data, you should protect your file transfers by using a secure protocol such as SFTP (SSH2) or FTPS (SSL). Ask your ISP if you can use SSH2 or SSL to transfer your files.