Troubleshooting a compromised cPanel account

Helpdesk Reports - 2026-07-09 - Security

Overview:

Security-compromised cPanel accounts can be very time-consuming and difficult to resolve and often require security expertise to resolve the issue along with web design to correct any impacts on your site, hence why we recommend cleaning them up.

Prerequisites:

Validate your IP address via the Micron21 WebAuth. For more information, you can review our WebAuth article here.

Method:

1. Perform ImmunifyAV Scan (Completed from WHM).
    1. Understanding which files are infected and when they became infected is the starting point.
2. Assess recovery from backup.
    1. This is the best way to recover from any compromise as long as you have back ups that predate the security compromise.
3. Check files from ImmunifyAV Scan.
    1. Remove each of the infected files or clean them up if possible.
    2. This can be very difficult and may mean that your site no longer works if critical files to the operation of your site are removed.
4. Update cPanel/Wordpress Passwords.
5. Update all plugins/themes.
6. Use Sucuri free scan for further investigation and a secondary review point.
    1. https://sitecheck.sucuri.net/ gives you an alternative scan assessment point to ensure that the site is most likely to be clean.
7. Use Sucuri paid scan and investigation to resolve fully.