Come posso vedere i files che mi avete segnalato come infetti?

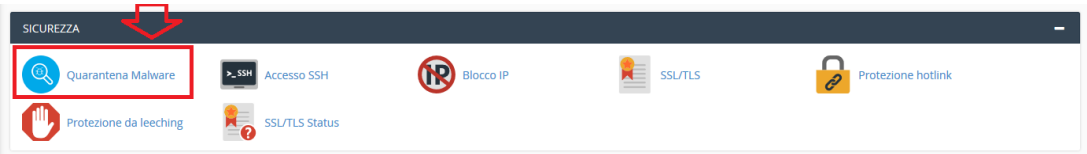
Mirko Pugliese - 2025-09-12 - Hosting cPanel

Per tutelare l'integrità dei nostri server e di tutti i siti web ospitati nella nostra infrastruttura, è attivo un antimalware per rilevare il codice infetto di tutti i file presenti nel server.

Il nostro sistema antimalware effettua, in tempo reale, la scansione di tutti i file che stai caricando nel Server via FTP (o da Filemanager del CPanel), infatti nel caso in cui dovessimo riscontrare del codice infetti l'upload di quel file verrà quindi immediatamente bloccato.

Ogni 15 giorni verrà effettuata una scansione completa di tutto il tuo account, così da garantirti sempre un servizio sicuro e privo di file infetti, infatti qualora dovessimo riscontrare del codice malevolo nel tuo applciativo, verrai informato dal nostro supporto tecnico che ti indicherà esattamente quali sono i file infetti.

Tutti i files ritenuti malevoli verranno spostati in "Quarantena" e sono da te consutabili dal CPanel nell'apposito tasto "Quarantena Malware", come dal seguente screen:



In questa pagina troverai tutti i file ritenuti malevoli, come di seguito:

Data rilevazione	Data modifica file	Nome file originale				
2016-02-12 17:17:00	2016-02-12 17:15:41	public_html/wp-content/tes4.php	Restore	Vedi	Download	Cancella
2016-02-12 17:17:00	2016-02-12 17:15:29	public_html/test2.php	Restore	Vedi	Download	Cancella
2016-02-16 11:26:16	2016-02-12 14:53:46	public_html/wp-conten.php	Restore	Vedi	Download	Cancella
2016-02-16 11:26:16	2016-02-16 11:25:04	public_html/test.php	Restore	Vedi	Download	Cancella
2016-02-16 11:36:06	2016-02-16 11:34:51	public_html/prova.php	Restore	Vedi	Download	Cancella
2016-04-01 14:46:16	2016-04-01 14:45:20	public_html/wp-content/tes3.php	Restore	Vedi	Download	Cancella
2016-04-01 14:46:16	2016-04-01 14:45:18	public_html/wp-content/tes1.php	Restore	Vedi	Download	Cancella
2016-04-01 14:46:16	2016-04-01 14:45:22	public_html/wp-content/tes4.php	Restore	Vedi	Download	Cancella
2016-04-04 12:13:58	2016-04-04 12:10:22	public_html/test_shell.php	Restore	Vedi	Download	Cancella
2016-04-04 14:28:52	2016-04-04 12:17:54	public_html/test_shell.php	Restore	Vedi	Download	Cancella
2016-04-04 15:07:02	2016-04-04 15:05:49	public_html/test_shell.php	Restore	Vedi	Download	Cancella
2016-04-04 15:48:35	2016-04-04 11:35:58	public_html/test_shell.php	Restore	Vedi	Download	Cancella
2016-04-04 15:52:09	2016-04-04 15:50:05	public_html/test_shell.php	Restore	Vedi	Download	Cancella
2016-04-05 10:57:08	2016-04-05 10:56:27	public_html/test_shell.php	Restore	Vedi	Download	Cancella
2016-04-06 09:53:52	2016-04-06 09:43:37	public_html/test_shell.php	Restore	Vedi	Download	Cancella

Come puoi vedere, hai la possibilità di effettuare 4 attività:

- Restore: questo ti permettà di ripristinare, in maniera del tutto autonoma, il file che è stato rilevato come infetto.

Prima di effettuare questa operazione è di fondamentale importanza essere certi che il file sia un "falso positivo", infatti uno script malevolo ricaricato nel tuo spazio potrebbe compromettere l'integrità del tuo sito web

- Vedi: questo ti permetterà di vedere in fondo alla pagina il codice malevolo che abbiamo trovato in quel file

- Download: questo ti permetterà di scaricare sul tuo PC il file infetto, così facendo potrai analizzare il codice e bonificarlo.

- Cancella: questa opzione cancellerà direttamente dalla quarantena il file rilevato come infetto.

Segnaliamo tutti i file infetti proprio per tutelare il tuo sito web e il tuo business, infatti ogni file malevolo può essere una falla di sicurezza sfruttata da qualche malintenzionato.