

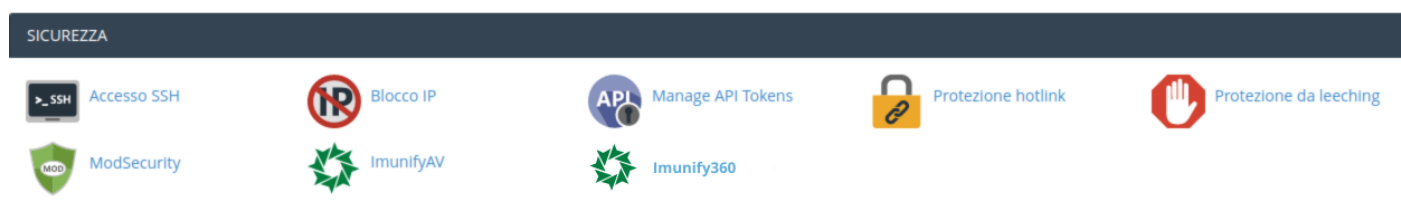
Imunify360 - cPanel

Imunify360 è uno scanner antimalware che rileva tutti i file dannosi, compresi backdoor, web-shell, virus, scripts, phishing e molti altri.

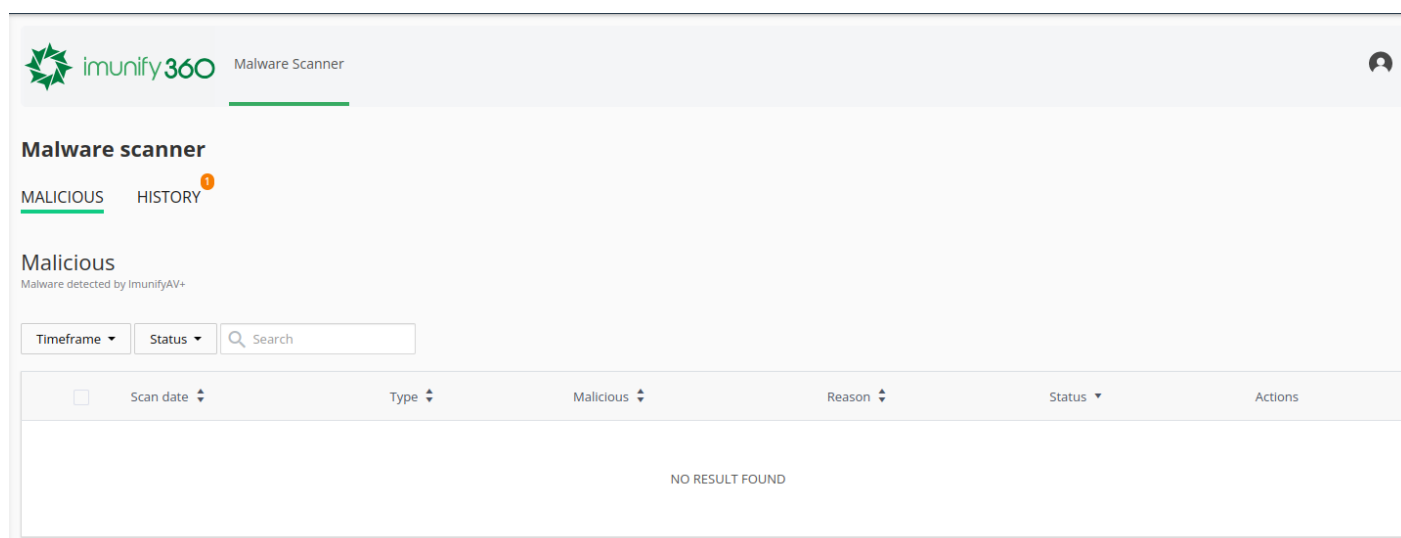
E' installato su tutti i server WHM di Artera e permette di gestire direttamente da cPanel i file che sono stati rilevati come dannosi.

In questa guida illustreremo come poter utilizzare le funzioni che il plugin Imunify360 mette a disposizione.

Prima di tutto è necessario accedere al proprio pannello di controllo visitando l'indirizzo <https://mail.DOMINIO:2083> con proprio browser internet, sostituendo a DOMINIO il dominio del vostro sito internet senza www, ed entrare nella sezione "Imunify360".



Una volta entrati il pannello mostrerà lo stato dei file contenuti nell'hosting a seguito dell'ultima scansione effettuata dal sistema. Nel caso in cui non sia stato rilevato del malware non verrà riportato nulla nella sezione Malicious.



Se invece sono presenti malware sotto la sezione Malicious troverete tutti i file che sono stati rilevati come infetti.

E' possibile eseguire due azioni sui malware rilevati:

- [View /home/esempiocom/public_html/b.php](#)

VJ1h3Zt3Zz2j1Ebkpsa1t6hAv1NVjJHtBtaSm51SWVET1ZDQ3s5SkhkhemhZwMdcRcPnRfQYnj3Rm3d3NHlWOXpOGs0GUkVWM2Z4RlBbDTzWldmbOtOeWQ1
 bJxAc3BMNmJmJcDd2b1IveWZteHNbY1tBdy9aNUjqbHrVm1ZsbkRVSG1wn2dBMzlvZ3c4dmgwbDhJWVA1M2lxVWRWR0hBtXRBUJlYlW1VfkrNkixMzgyZU5e
 emM2bWbhnWu5uRuS0eR29bH3p3MwdrTFyL1krTWwrT9i9avJzGdsVlRWMdZemNmNQyV9BZvpqVWR1T59HukQzU21cxdj3L1F0S21TUVa3UzjMSDjTE15N0M3
 blAxZzhL0UxaytBM25NySGKZ256TUzPbTcM2r1ZdtTndweTVWYvDubXfMEdHmQVZTNXGkdVNXU2RyAWhaUkzSjVwRS9jTJXNS50PtzcEvcUxWbHplRIdaRjdz
 VFVSNUQ5UE5SeEwxN1ZoYVWmSEXYbDh5v5Cm2R3h7ZmwybXkXBVglVYHtJK3dva2hXGdM3A3vb2Vht2TfmcnlvQ0VbFVBJV3MHZKnlJlTlEwRjz1dBSkZr
 bkdUdUYrU0t2NtYB0rmloaXVuRHVkyVBzNUxVVMxvDlMv6K1Yy5m5M5WURSeFVRZBUQ1ZZYnlnNRGQRnU93cVl5YwVrV1JlaDMrRFBhMlhwTww5MWZaWDhI
 NWpQTG5GbnYRQV9mCwXw1t5fM1NzVzb3JmXksva3dwdFZV51RteDdoEdlDRStyK1krbEzEBlWMJl0S2dNtHbW5UL1BrCZCTKu0QxpK0XGTvc1WHU5NFY0
 NVNqgUpZkPqXGbu5m5sThsQjCtPlbTzF3skNwdFtQLlxRmp9dHhVhRvYVWdZSEVhZUvZn0NtHlWt3Z3FXUE9XeqZvdNb3hAvJcy3c3Nbm5MavdY
 YnyVwVVCY2RPK1Nsvm1mNU9jRnj5CwJYk1ZanAwOHhGc21a1MxM01hWGDqTJBWmVndUeG5jYmFmsSzc2z1mZlWblBVumpOclRoenpuZCjNqNmvdGU2c3o3
 dzNRmNlzenN2dc1cWw2NTZNWmluOVdbw21DrlN6eG5QWwHBRM1Jf3h3d63pNYZMr3hGeU9CUElocFRkBl0kaGvYU2t3kXqU5XL2NnM2tznRTNHWtAYU0Y0
 tYwWkVwVIRMOFYOEQ5SbmBoZnLCSHNrmhY5mt3QWlzb0ZhZmFubNhmOTfIveCtdkcoz254MjRfFOWky1JxThxU1t4VURITWxGL1hWaTJsL2U4VUDFRTN2
 VnhIMidOWtmNEFQJTSBmW0L3XUC9NSxdmbWlKfRRdKlJWwQrck21dJhXUeRuoaqFVQMxdtdKOENSKvRnzJda1Y1Yzvc2tByRlroyTRshdUpUOtztch1o
 LytndE9RcWp6R0qV0Z5ejE3V1ZChU0xV1A3efYfYbFkxeWNieFVZDJMa2ZOEOjVtYUrmjMkFqJUVRub0F5dzhjNGFFWAFhAcvYUkEg4MFCVSwnhWlN2
 V1CbW5U0M2d6Y2UwSmXMEg1dvJjaE2VZmpkb1NkAkxERwFz3M3yMwVGFUZM20jtUkx5b2doa2dBV29VQJZUwXZPNG0sZOZ5YsLQ2p6M0dzak560StBmm04
 eWg3bFFWOC0u53ZCT2R9m9QXZCbUldUdJRGEEvKbXSDvcmrMnpGmJvxvQzWQ2RPRIFlV949eARERvZuA8X3K9a3w3pmsyUuVnMnNBtmNd
 QW8wTfJQaUxodmFFNVR1clvKRFdIUUQ2MDJ2aHp4YkFvN0j1dgnQwVgV1Y0lHek5Cd3RvU1g4OHZ0T2tJZFgzM1I3M0k3MEdkmFHY28rc0kwajZBdUfIUFEU5
 L0txbFWRGh90V3NVZGhuemVzkZ5UDTMFOm01NFZxbTdvMFvIZ9YdZ8L040VwldVgWvdTWSExp0S9wR3dyWktrQTvJazQndXmM21UR1c5bURoem9plbVE4
 N2RtUXfKCG90dHNCMTYEOE1VXF6RlPUWVIOHF4bjojnJdcbk9Z2FOZUL2anp0OWfBzjNmS21EzkkzdUldhLknpNQRtQQRGRUfTwcBdLl9a9qm35NnRjdtFV
 QXVqb3pRyRSUHuXOTFNQXUkFpPdrFQUvh3hGjJMNUE4vYv3KfmlU2tFGZULsWxh2ZjdZdGz0Vj13NZ2WU0reTgra3I4dGFUDFvGadG4FpCb1VBZGvm
 L1N4tZrYkL52JoUGxraopk1B4RG5Xe4E03hXkCldEUxvMq3OWEz2dXBiyNpWakRud1pxdD0cJlJazB0ZtQJQlJEM5CWERVdFhwYTAzavhVeEJENKZG
 K1q1aQdZLRlFad25mQrClcGjYUuW5rUVRFC3pWYtYtJ3aVudmhqN5UtaUNRGdVjV0GPN5SG83UXNkeVc0Wk3pCEyzeVfsczRoK5XQ1FPYlJZNUEnVenF
 cT2W1ZtEaNT2m9WntBuN1YUNkRlCElOYVRV1MSMtu5U5EtR2c38bZuXQxYZwchL2dkl2YU14L17sZ1NIZVFZ3hac0FzCkN0RfBZ20RlanBPQWnhBkyE

- Con il tasto riportante l'icona "scopa" è possibile ripulire il file infetto.

Clean up malicious code

/home/esempiocom/public_html/b.php

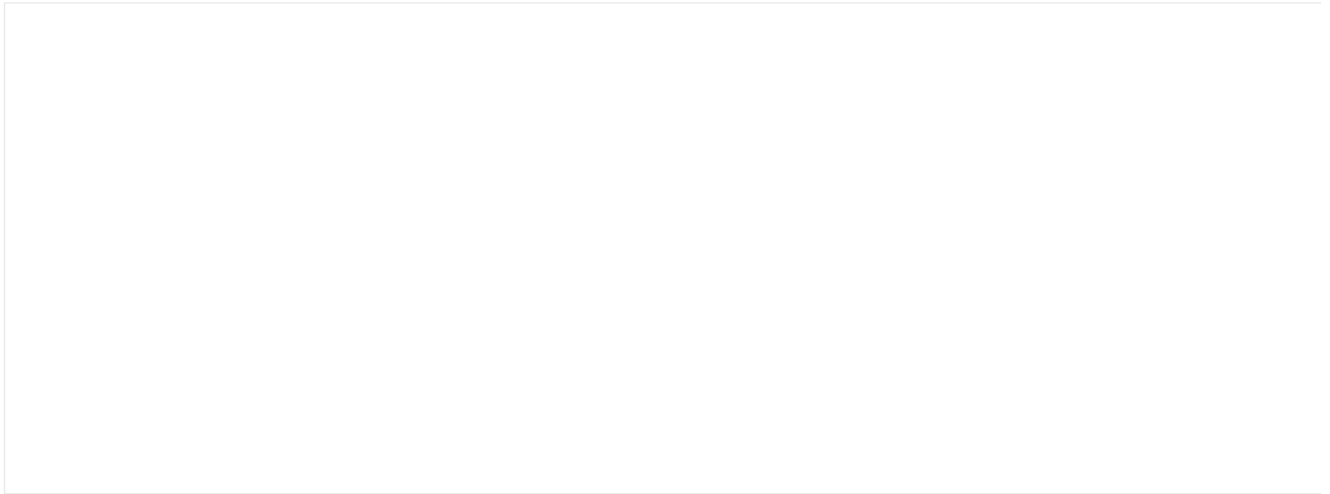
Come indicato nel popup che compare procedendo con la pulizia del malware, il backup del file originale rimarrà disponibile e recuperabile per 14 giorni, dopodiché sarà rimosso.

Una volta ripulito il file verrà visualizzato come segue.

A questo punto sarà possibile eseguire due operazioni su di esso:

- con il tasto riportante l'icona "occhio" sarà sempre possibile visualizzare il contenuto del file, ma in questo risulterà ripulito dal codice malevolo

View /home/esempiocom/public_html/b.php



CANCEL

- con il tasto riportante l'icona "orologio" sarà, invece, possibile ripristinare il file originale, operazione necessaria nel caso il sistema dovesse rimuovere anche del codice essenziale per il corretto funzionamento del sito.

Restore (possibly infected) copy made before a cleanup attempt



/home/esempiocom/public_html/b.php

CANCEL

YES, RESTORE

Sotto la sezione History sarà possibile visualizzare lo storico delle operazioni effettuate sui file malevoli.



Malware scanner

MALICIOUS HISTORY

History

Date ▲	Type ▼	Path ▼	Cause ▼	Initiator ▼	Event
April 28, 2022 11:10 AM		/home/esempiocom/public_html/b.php	manual	root	Restored original
April 28, 2022 11:10 AM		/home/esempiocom/public_html/b.php	manual	root	Cleanup removed content
April 28, 2022 11:08 AM		/home/esempiocom/public_html/b.php	manual	root	Restored original
April 28, 2022 10:53 AM		/home/esempiocom/public_html/b.php	manual	root	Cleanup removed content
April 25, 2022 8:00 AM		/home/esempiocom/public_html/b.php	background	root	Detected as malicious
April 20, 2022 4:37 PM		/home/esempiocom/public_html/b.php	user	root	Detected as malicious

Items per page: 25 ▼

Revision #10
Created 20 April 2022 14:41:26 by Riccardo Falsetti
Updated 12 December 2024 10:09:00 by Alessia Rossi