

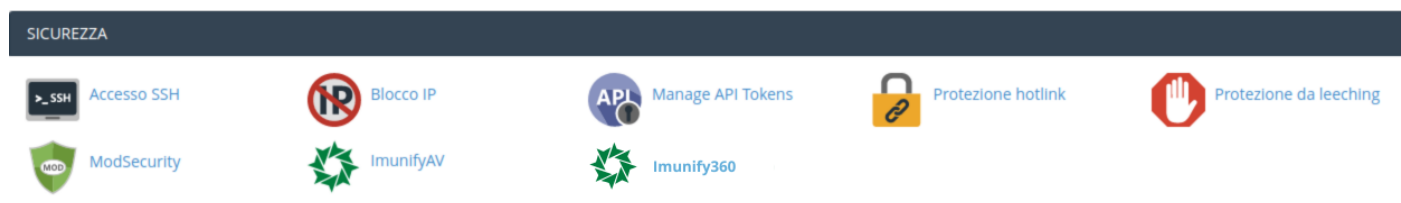
Imunify360 - cPanel

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

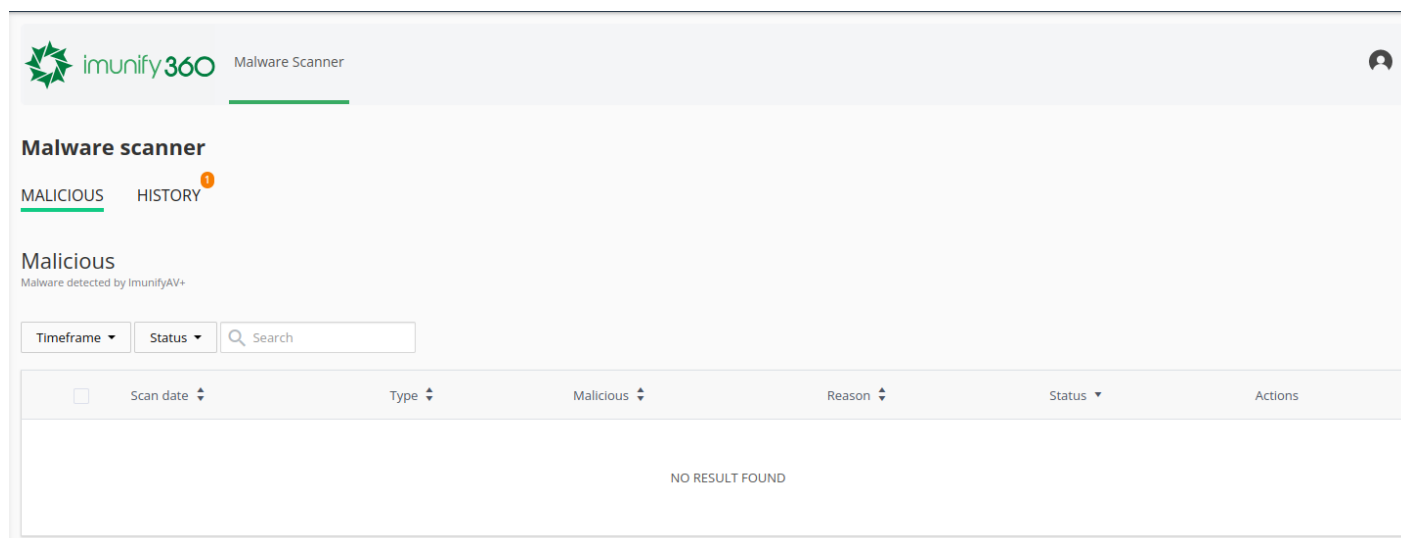
E' installato su tutti i server WHM di Artera e permette di gestire direttamente da cPanel i file che sono stati rilevati come dannosi.

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](#)

VJ1h3tZ3Zz21Jebkpsa1h6aV1NVJjH0TbASm11SWVET1ZDQ3s5SkhkhemhZwMdcRcPnRfdQYnj3Rmd3NHlWOXpOGs0Gsu0KvWM2Z4RlBbDTzWldmbutOeWQ1
 bJxAc3BMNjmJclDd2b1IveWZteHNbY1dBdy9ANuJqBhRvM1ZsbkRVSG1wn2dBZmlvZ3c4dmgwbDhJWVA1M2lxVWRWR0hBtXRBUJlYlW1VfkrNkixMzgyZU5e
 enM2bWbhnW5uSuRu0S292bH3p3MwdrTFyL1krTWwrT9IvaVujZGdsVlRWMldZemNqYv9BZvpqVWR1T59HukQzU21cxdj3L1F0S21TUVa3UzJMSDjTE15N0M3
 blAxZhL0UxaytBM25NySGKZ256TUPbTcM2rZdTwndweTVWYvDubXfMEdHmQVZTNXGkdVNXU2RyAWhaUkzSjVwRS9JTzNS50PtzcEvcUxWbHplRIdaRjdz
 VFVSNUQ5Ue5SeEwxN1ZoYVWmSEXYbDh5cV5M2R3hYzmywbXbVblgVYjTK3dva2hXGdM3A3vb2Vht2FmclnQv0VbFVEVj3MHZKnlJlTlEWkrJ1d8SkZr
 bkdudUYrU0t2NtYRGmloaXVuRHVkyVBzNUxVVMxvDlMv6K1Yy5m5M5WURSeFVRZBUQ1ZZYnlnNRGQRnU93cVl5YwVrV1JlaDMrRFBhMlhwTww5MWZaWDhI
 NWpQTG5GbnYbQ9m9cawx5HsMlZvb2JmXksva3dwdFZV51RteDdoEdlDRStyK1krbEzEBlWMJl0S25HlNhbW5UL1BrCZCTKu0QxpK0XGTvc1WHU5NFY0
 NVNqgUpZkPqXGbu5mw1t0fJCtPlbTzF3skNwdFtQLlxRmp9dHhVhRvYVWdZSEVhZUvZn0NtHlWf3ZC3FXUE9XEQvdNb3haVjcy33Nbm5MaVdy
 YnyvVVCY2RPK1Nsvm1mNU9jRnj5CwJYk1ZanAwOHhGc21a1MxM01hWGDqTJBWmdVndUeG5jYmFmsSzc221mZlWblBVumpOclRoenpuZCjNqMvdGU2c3o3
 dzNRmInzenN2dc1cWw2NTZNWmluOvdbw21DrlN6eGSQWHBHM1Fuj3d6d3pNYZMr3hGeU9CUElocFRKb0lkaGe0YTU23kXqU5XL2NnM2tznRTNHWTAyU0Y0
 tYwWkVwVlRMOFYOEQ5SbmBoZnLCSHNrmhY5mt3QWlzb0ZhZmJfNBhnmOTfIveCtdkocz254MjRfFOWky1JxThx01V4VURITWxGL1hWaTJsL2U4VUDFRTN2
 VnhIMidOWtmNEFQUTSBMw0ZnL3UC9NSxdmbWlKfRRdKlJWwQrck21dJhXUeRuoaqFVQMxdtdKOENSKvRnZJda1Y1Yzvc2ByRlroyTRshdUpUOTzhtc1h
 LytndE9RcWp6R0qvQZ5eJ3V1ZChUoxV1A3efYfYfKkeWnieFVZDJMa2ZOEOjvTYrYmjMfCjqlUVRub0F5dzhjNGFFWAFHAcHcvYUkTEg4MFVC5WnHwIN2
 V1CbW5U0M2d6Y2UwSmXMEg1dvJjaE2V5Zmpkb1NkAkxERwFzM3hYmVWGFUZM20JtUkx5b2doa2dBW29V9QJ1VwZUJXZPNG0sZ0Z5YsLQ2p6M0dzak560StBmm04
 eGx3bFFWOC0v53ZCT2R9m9QZCblUuYdJlRGJEeXbKSDvcmorMnpGjVxcvQZwQ2RPRIFlwV949eARSEdRvAu8X3K3ra2p3sm5yUuVnMnNBtmNd
 QW8wTfJQaUxodmFFNVR1clvKRFdIUUQ2MDJ2aHp4YkFvN0j1dgnQwVgY1Y0lHek5Cd3RvU1g4OHZ0T2dJZFgzM1I3M0K3MEdkamFHY28rc0kwajZBdUfIUFEU5
 L0txbFWRGh09V3NVZGhuemVzkZ5DUTFM0c1NFZxbTdmFViZi9Yd28ZL040VmlVdGvwdTVSExp0S9wR3dyWktrQTvJazQndXmM21UR1c5bURoem9plbVE4
 N2RtUXFKEG90dHNCMTYOEZ1VXF0RkPUWVIOHF4bjoJnJdYbk9Z2FOZUL2anp0OWfBzjNmS21EzkkzdUllhdkNP0QTRQGRUhtFWcDbL0I9amQ95NnRjdtFV
 QXVqb3pRyRSUHuXOTFNQXubFpPdrFQUvh3hGjJMNUE4vCbV93KcmU2tFGZULsWxh2Zjd2GdZ0Vj13NZ2WU0reTgra3I4dGFUDFvGadG4FpCb1VBZGvm
 L1N4tZrYkL52JoUGxraopk1B4RG5Xe4E03hXkCldEuxXvMq3OWEz2dXBiyNpWakRud1pxdD0cJlJazB0ZJQJlEM5CWERVdFhwYTAzavhVeEJENKZG
 K1q1aQdZLRlFad25mQrClcGjYUuW5rUVRFC3pWYtYtJ3aVudmhqN5SutaUNRGdVjV0GPN5SG83UXNkeVc0Wk3pCEyzeVfsczRoK5XQ1FPYlZNUEnVenF
 cT2W1ZTEntZm9wNtBuN1YUNKRLcEJOYVRV11MSUtMsU25UrEz238BuZnOXqYZwchL2dkl2YU14L17sZ1NIZVFZ3hac0FzKnoNRfB2Z0RlanBPQWbnBky

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

Clean up malicious code

/home/esempiocom/public_html/b.php

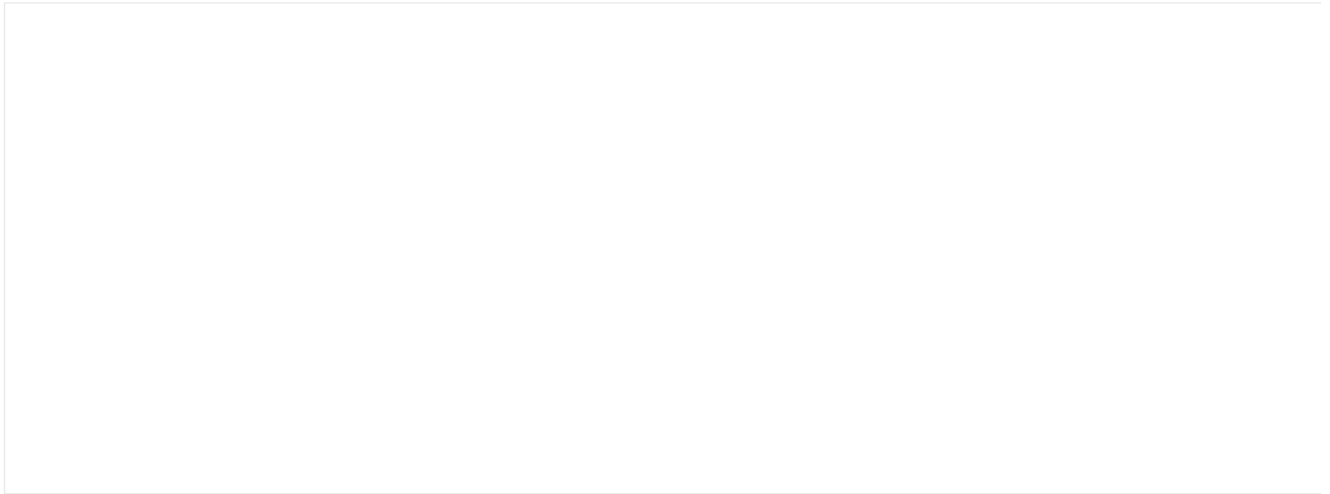
Come indicato nel popup che compare procedendo con la pulizia del malware, il backup del file originale rimarrà disponibile e recuperabile per 14 giorni, dopodiché sarà rimosso.

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

 Search

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