

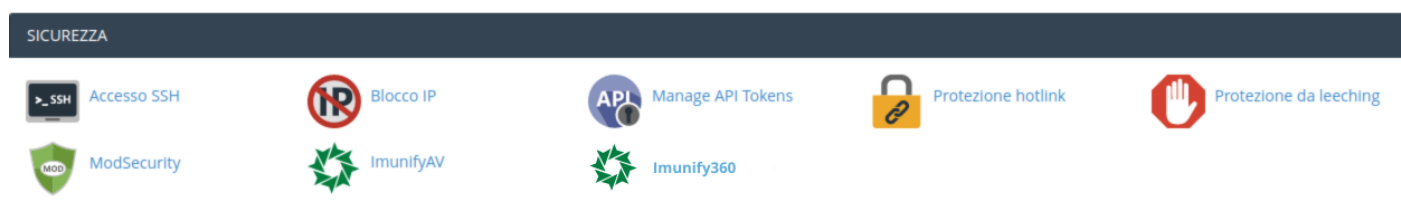
Imunify360 - cPanel

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

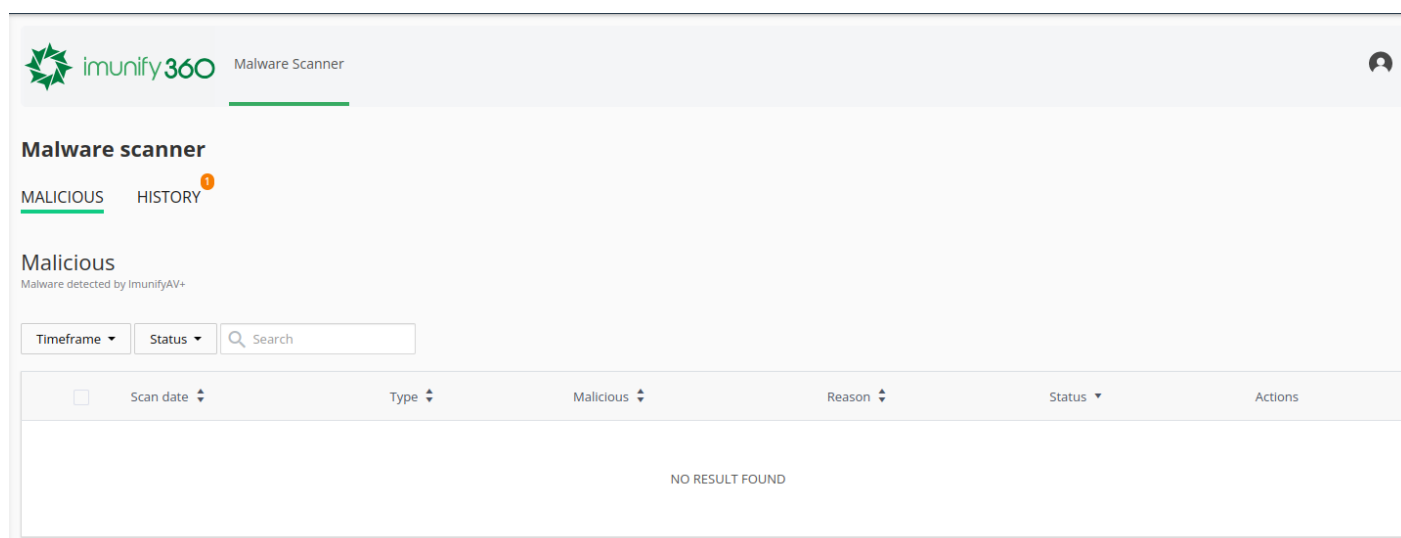
E' installato su tutti i server WHM di Artera e permette di gestire direttamente da cPanel i file che sono stati rilevati come dannosi.

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](#)

VJ1h3tZ3Zz21Jebkpsa1h6aVh1NVJHQTbSa5m11SWVET12DQ35SkshkhemhZwMdcRcPnRfQYnj3Rm3dNHlWOXpOGs0G5uKwVMW2R4RlBbDTzWldmbutOeWQ1
 bJxAc3BMNjmJcDd2b1IveWZteHNbY1dBDy9aNUjqbHrVm1ZsbkRVSG1wn2dBMzlvZ3c4dmgwbDhJWVA1M2lxVWRWR0hBtXRBUJlYlW1VfkrNkixMzgyZU5e
 emM2bWbhnW5uSuRu5O292bHp3MwdrTFyL1krTWwrT9i9avJzGdsVlRWMDZemNqYv9BZvpqVWR1T59HukQzU21cxdJ3L1F0S21TUVa3UzJMSDJTE15N0M3
 blAxZhL0UxaytBM25NySGKZ256TzPbTcM2r1dTwndTeWYvDubbXfMEdHmQVZtNXGkdVNXU2RyAWhaUkzSjVwRS9JTzNS50PtzcEvcUxWbHplRIdaRjdz
 VFVSNUQ5Ue5SeEwxN1ZoYwWwSE5XyDb5v5Cm2R3h7ZmwybXkXBVglvYHJT3kda2hXGdM3A3vb2Vnt2FmcnlvQ0VbVFEVJ3MHKZnjL1TlEWkrJ1d8SkZr
 bkdudUYrU0t2NtYB0rmlaoXVuRhVHVkYBzNUxvVVMxcDlVwM6K1Yv5m5M5WUR5eFVRZBUQ1ZZYnlnNRGQRnU93cVl5WrcV1JlaDMrRFBhMlhWtWw5MWZaWDhI
 NWpQTG5GbnYQV8g9cWw5tH5fM1CvXmKsva3dwdFZV51RteDdoEdlDR5tYk1krbEzEBlWlJW0S2dNt1NhbW5UL1BrC2CTKu0QxpK0XGTvc1WHU5NFY0
 NVNqgUpZkPqXG8uB5w10sQ1CtPlbTzF3skNwdFtQLlxRmp9dHhVhRvYwWdZSEVhZUvZn0Nt1HhW3Z3FXUE9XEQvdNb3haVjcy33N5mMaVdy
 YnyvVVCY2RPK1Nsvm1mNU9jRnj5CwJYk1ZanAwOHhGc21a1MxM01hWGDqTJBWmdVndUeG5jYmFmsSzc221mZlWblBVumpOclRoenpuZCjNqMvdGU2c3o3
 dzNRm1nZenN2dc1cWw2NTZNWmluOvdbw21DrlN6eG5QWwHBRM1Jf3b3d63pNY2Mr3hGeU9CUElocFRkBl0kaGvYU23kXqU5XL2NnM2tznRTNHWtAYU0Y0
 tYwWkVwWlRMOFYOEQ5SbmBoZnClSHNNRmhY5mt3QWlzb0ZhZmFubNhmOTfIveCtdkcoz254MjRfFOWky1JxThxU14VURITWxGL1hWaTJsL2U4VUDFRTN2
 VnhIMidOWtwnNEFQUTSBMw0Zn3XUC9NSxdmbWlKRFKRdEJlWJWQrck21dJhUxRUoaqFVQXmxdtKdOENSKvRnZJda1Y1Yzvc2ByRlroyTRshdUpUOtztch1o
 LytndE9RcWp6R0qV0Z5ejE3V1ZChU0xV1A3efYfYbFkxeWNieFVZDJMa2ZOEOjVtYrYmjMfCjqlUVRubO5fdzhjNGFFWAFHAcHcvYUkTEg4MFVC5WnHwIN2
 V1CbW5UWMD26Y2UwSmXMEg1dVJJaE2V5Zmpkb1NkAkxERwFzM3hYmWVGUFZM20JtUkx5b2doa2dBW29V9QJ1VwZUxPNG0xZOZ5YsLQ2p6M0dzak560StBmm04
 eWg3bFFWOC0x5ZCT2R9m9QXZCblUdUJDRGEzE5K5DwcmrMnpG6JvxzcQWZRPRIFLV949eARERZV8uA8X3K9a3w3pmsyUuVnMnNBtmNd
 QW8wTfJQaUxodmFFNVR1clvKRFdIUUQ2MDJ2aHp4YkFvN0j1dgnQWVg1Y0lHek5Cd3RvU1g4OHZ0T2dJZFgzM1I3M0K3MEdkmFHY28rc0kwajZBdUfIUFEU5
 L0txbFWRGh90V3NVZGhuemVkZ5UDTvmF0K1NFZxbTdmFViZi9YdZ8L040VwldVgWvdTW5Xexp0S9wR3dyWktrQTvJazQndXmM21UR1c5bURoem9plbVE4
 N2RtUXFKCG90dHNCMTYEOE1VXF6RlPUWVIOHF4bjoJnJdvk9Z2FOZUL2anp0WFbZjNmS21EzkkzdUllhkdNpQTRQOGRUhtFWcDbL0I9amQ95NnRjdtFV
 QXVQb3pRyRSUHuXOTFNQXU5bFpPdrFQUVh3hQJmJNUe4CbV3Y3KcmU2tFGZUL5Wxh2ZjdZGdZ0Vj13NZ2WU0reTgra3I4dGFUDFVdGad4FpCb1VBZGvm
 L1N4tZrYkL52JoUGxraopK1B4RG5Xe4E03hXkCldEUxvMq3OWEz2dXBiyNpWakRud1pxdD0cJlJazB0ZJQJlEM5CWERVdFhwYtAzaVhVeEJENKZG
 K1q1aQdZLRlFad25mQrCJGjYUxU5W5rVVRFC3pWYtYtJ3aVudmhqN5U5UtaNURGdVjV0GPN5SG83UXNkeVc0Wk5pCEyeZvFsczRoK5XQ1FPYJZNUEnVenF
 cT2W12TEntZm9wNTBuN1YUNKRLCtEJOYVRV1MSMtu5U5EtR2c35BzU2XoXyZwchL2dki2YU14L17sZ1NIZVFZ3hac0FzKNoNRfBZ20RlanBPQWbnBky

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

Clean up malicious code

/home/esempiocom/public_html/b.php



Original backup will be available for 14 days after cleanup was performed. You'll see "Cleaned" and "Removed" items in the Malicious Files table until that backup is removed.

CANCEL

YES, CLEAN UP

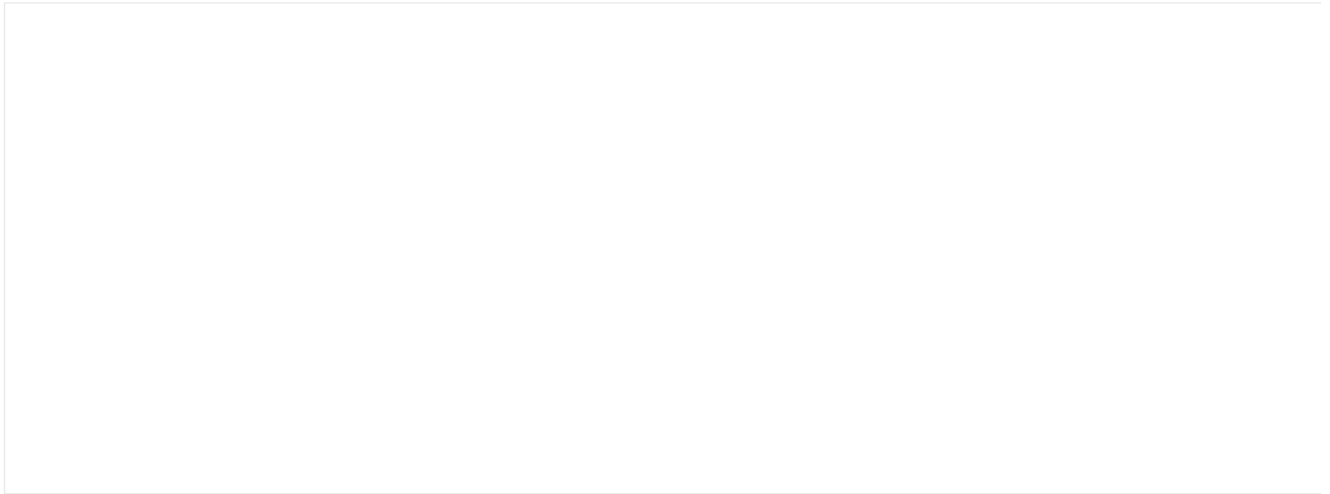
Come indicato nel popup che compare procedendo con la pulizia del malware, il backup del file originale rimarrà disponibile e recuperabile per 14 giorni, dopodiché sarà rimosso.

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