

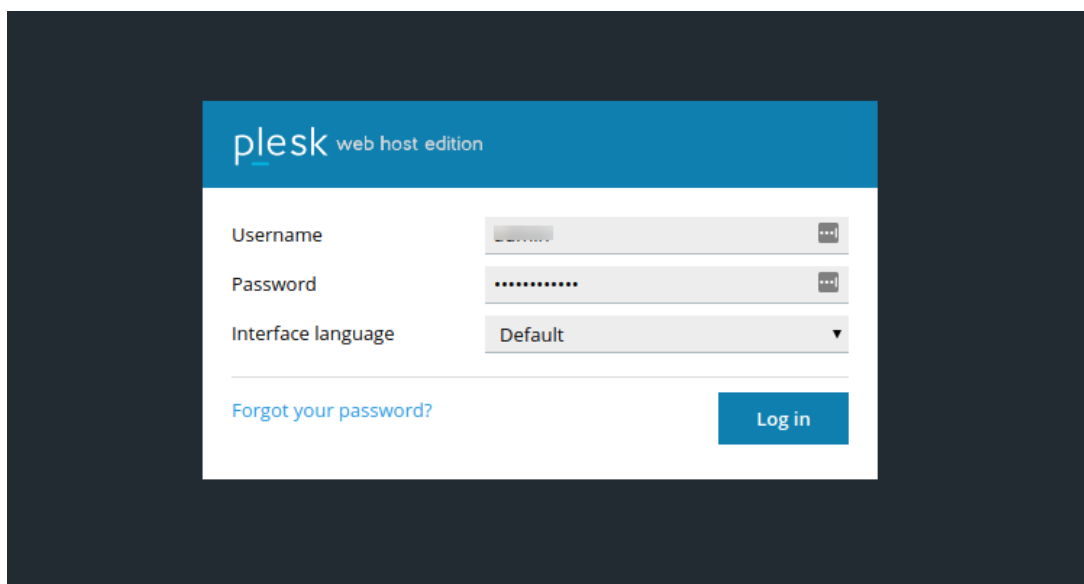
Γνωσιακή βάση > Plesk > Άλλες > Πως μπορώ να καθαρίσω με το ImunifyAV το κακόβουλο περιεχόμενο της σελίδα μου σε Bing Bang πακέτο φιλοξενίας;

## Πως μπορώ να καθαρίσω με το ImunifyAV το κακόβουλο περιεχόμενο της σελίδα μου σε Bing Bang πακέτο φιλοξενίας;

Ioanna Anifanti - 2019-11-27 - Άλλες

Σε περίπτωση που έχετε **Bing Bang** πακέτο φιλοξενίας, εκτός από [σκανάρισμα των αρχείων](#) σας για τυχόν ύπαρξη κακόβουλου υλικού, έχετε τη δυνατότητα να πραγματοποιήσετε και άμεσα **καθαρισμό των μολυσμένων αρχείων**.

Για να πραγματοποιήσετε την διαδικασία αυτή, θα χρειαστεί αρχικά να συνδεθείτε στο Plesk με τα στοιχεία πρόσβασης σας.



Στη συνέχεια, έχοντας επιλέξει από την αριστερή λίστα το **Website & Domains** κάνετε click στην επιλογή **ImunifyAV**.

imunifytest.linuxzone79.grserver.gr

Website at <http://docs/> IP address: 88.99.166.170 System user: imunifytest

Hosting Settings Open Preview Suspend Disable Description

Start creating your website in one of the following ways:

**WordPress**  
Create your website using WordPress.

Install WordPress

**Install an Application**  
Create your site by installing a web app, such as Joomla or Drupal.

Install Apps

**Create a Custom Website**  
Upload your web content and add databases.

Files Databases

SHOW LESS

Web Hosting Access

FTP Access

Hosting Settings

Git

Let's Encrypt

Node.js

Ruby

PHP Settings  
PHP version: 7.3.11

Apache & nginx Settings

Applications

File Manager

Mail Importing

Website Importing

Web Statistics

Web Statistics SSL/TLS

DNS Settings

Email Addresses

Mail Settings

Limit Outgoing Messages

SSL/TLS Certificates

Web Application Firewall

Password-Protected Directories

Website Copying

Logs

Web Users

Advisor

DNSSEC

ImunifyAV

Εφόσον πρώτα έχετε τρέξει το **Scan** στα αρχεία σας, σας εμφανίζεται η αναφορά του ImunifyAV με τα αρχεία που περιέχουν τυχόν κενά ασφαλείας ή malware, όπως φαίνεται στην παρακάτω εικόνα.

Back to Administrator Logged in as: ilias.kipress Subscription: imunifytest.linuxzone79.grserver.gr Advisor Help

### Scanning Report

Scanned Folder /var/www/hosts/imunifytest.linuxzone79.grserver.gr/httpdocs

The website seems to be compromised and infected. Try to clean it automatically using the "Clean Malware" button or request a manual malware cleanup service by security experts.

Number of detected malicious files: 1, click the button below to clean them automatically.

[Clean Malware](#) [Back to reports](#)

**Summary**

Finished at: 2019-11-12 11:34:29  
Spent time: 2m55s  
Number of scanned files: 24198  
Available for auto-cleanup: 1

ID	Type	Action	Signature ID	File	Size	Modified
1	SRV	Ignore	SMW-SA-05014-miw.perl-0	<a href="#">js/calendar/crazy.pl</a> ...[pentrawe*PASTP* S1]R[isAdmin]EricU&ktmgw/*P[rick]-y[pen]traw&qu...	138 KB	2019-02-13 14:38:52

1 items total

[Whitelist Management](#)

**Quick Help**

Files listed above are malicious. There are two kind of malware: server malware and client malware. It could be identified in the report according to the icon in the "type" column.

- SRV** — Server malware is usually hacker's backdoors, web-shells, malicious injections in the files, spam mailers, doorways and hacker's tools. Usually it is located in the files written in php, pl or python.
- CU** — Client malware is mainly javascript injections in the .js files, templates or php scripts. It usually affects user experience on the page, e.g. redirects user or performs a hidden load of some malicious code in a browser.
- |** — The marker shows the beginning of malicious code in a file.

Για να αφαιρέσετε αυτόματα αυτά τα μολυσμένα αρχεία που εντοπίστηκαν, επιλέξτε **Clean Malware**.

## Scanning Report

Scanned Folder /var/www/vhosts/imunifytest.linuxzone79.grserver.gr/httpdocs

! The website seems to be compromised and infected. Try to clean it automatically using the "Clean Malware" button or request a manual [malware cleanup service](#) by security experts.

Number of detected malicious files: 1, click the button below to clean them automatically.

Clean Malware

Back to reports

Αφού ολοκληρωθεί ο καθαρισμός από το ImunifyAV, εμφανίζεται η αναφορά με τα αρχεία που καθαρίστηκαν και συγκεκριμένα στην στήλη **Action Status** αναφέρεται το κατάσταση των αρχείων μετά τον καθαρισμό.

Domain	State	Report Time	Actions	Action Status
imunifytest.linuxzone79.grserver.gr ..linuxzone79.grserver.gr/httpdocs	Clean	2019-11-12 11:34:29	Scan Clean Undo View Report	Cleaned 1 file

Customers knowledge base and interface description: <https://plesk.revsium.com/help/>.

Click the buttons next to the website:

- "Scan" — to scan website's files for malware.
- "Clean" — to cleanup detected malware automatically (available in Premium version).
- "Undo" — to restore original files before malware cleanup and
- "View Report" — to see the list of infected or cleaned files.

Check the report for domain blacklist status details.

Το ImunifyAV θα διατηρήσει το site σας λειτουργικό και μετά την εκκαθάριση κακόβουλου λογισμικού. Πιο συγκεκριμένα, διατηρεί τα πρωτότυπα αρχεία για χρονική περίοδο 7 ημερών στον φάκελο αντιγράφων ασφαλείας, ώστε να μπορείτε να επαναφέρετε τα αρχικά αρχεία όπως ήταν πριν από την εκκαθάριση κακόβουλου λογισμικού, μέσω του κουμπιού **Undo**.

## Actions



Scan



Clean



Undo



View Report

Μια εναλλακτική επιλογή που έχετε σε περίπτωση που επιθυμείτε να καθαρίσετε το site σας από τυχόν κακόβουλο λογισμικό είναι να χρησιμοποιήσετε την **Υπηρεσία Cleanup**, για να αφαιρέσετε τους ιούς και να προστατεύσετε το site σας από μελλοντική μόλυνση. Η Υπηρεσία Cleanup πραγματοποιείται από ειδικούς ασφαλείας της Top.Host και το μόνο που χρειάζεται από την πλευρά σας είναι [να επικοινωνήσετε με το τμήμα υποστήριξης](#) για την ενεργοποίηση της υπηρεσίας αυτής.