

DNS & IP BLACKLIST

Cosa fare in caso un indirizzo IP finisce in una black list pubblica



Comprendere il problema

01

Siti web creati con CMS (non in SaaS) sono **molto diffusi** e con molti plugin sono continuamente soggetti ad attacchi informatici.

02

Spesso questi siti sono ospitati su **VPS** auto gestiti dal cliente stesso senza **nessun tipo di sicurezza**, ad esempio nessun limite di invio email.

03

Sono estremamente diffusi attacchi con cui un sito web viene usato per inviare email di spam (o per ospitare un sito clone di altri siti noti - phishing). Un attacco **phishing** infatti è efficace in combinazione fra **spam + sito clone**.

Esempi di VPS a basso costo.

The screenshot shows the OVHcloud website's VPS pricing page. It features four plan cards against a blue background with a geometric pattern:

- VALUE**: **5€ +IVA/mese**, **4,60 €** (cioè 5,61 € IVA incl./mese). Includes 1 vCore, 2 GB, 40 GB SSD NVMe, and 250 Mbps illimitato*. [Ordina adesso](#) button. [Scopri di più →](#)
- ESSENTIAL**: **10€ +IVA/mese**, **9,20 €** (cioè 11,22 € IVA incl./mese). Includes 2 vCore, 4 GB, 80 GB SSD NVMe, and 500 Mbps illimitato*. [Ordina adesso](#) button. [Scopri di più →](#)
- COMFORT**: **20€ +IVA/mese**, **18,40 €** (cioè 22,45 € IVA incl./mese). Includes 4 vCore, 8 GB, 160 GB SSD NVMe, and 1 Gbps illimitato*. [Ordina adesso](#) button. [Scopri di più →](#)
- ELITE**: **A partire da 30 € +IVA/mese**, **27,60 €** (cioè 33,67 € IVA incl./mese). Includes 8 vCore, 32 GB, 640 GB SSD NVMe, and 2 Gbps illimitato*. [Ordina adesso](#) button. [Scopri di più →](#)



Mancanza di sicurezza

La sicurezza manca perché:

- 1) Nel CMS che ha continuo bisogno di aggiornamenti. Essendo il CMS **diffusissimo** ed il **codice open**, ci sono moltissime possibilità di trovare un bug e quindi è soggetto spesso ad attacchi.
- 2) **VPS senza limiti di invio posta**: spesso queste VPS non hanno controlli, proprio perché spesso usati come ambiente di sviluppo.

Molte vulnerabilità

Le vulnerabilità nei CMS sono talmente diffuse che si trovano tantissimi siti dove descritto come poterli attaccare, ma si trovano molti tools già integrati ad esempio anche nei tools presenti nel diffusissimo banalmente in kali linux (ex Backtrack) .

The image shows three screenshots of web-based security tools:

- CVE Details:** A search interface for security vulnerabilities. It includes a search bar, a sidebar with navigation links like "Home", "Vendors", "Products", and "Vulnerabilities By Date", and a main table showing results for "Wordpress > Wordpress : Security Vulnerabilities". The table columns include CVE ID, CWE ID, # of Exploits, Vulnerability Type(s), Publish Date, Update Date, Score, Gained Access Level, and Access.
- EXPLOIT DATABASE:** A search interface for exploit details. It features a sidebar with filters for "Verified" and "Has App", and a main table listing exploits by date, title, type, platform, and author. Examples include "n-Notes 1.6.2 - Denial of Service (PoC)" and "Sticky Notes Widget Version 3.0.6 - Denial of Service (PoC)".
- patchstack Vulnerability Database:** A search interface for vulnerability details. It shows a table of vulnerabilities across two tabs: "SOFTWARE" and "VULNERABILITY". The table includes columns for name, severity (e.g., 5.4), and type (e.g., Plugin). Examples include "WordPress WC Marketplace plugin <= 3.7.3 - Cross-Site Request Forgery (CSRF) vulnerability" and "WordPress Qtranslate Slug plugin <= 1.1.18 - Cross-Site Request Forgery (CSRF) vulnerability".



Cosa succede se si finisce
in black list?

1) Si sparisce dalla SERP di
GOOGLE

2) Non si riesce più ad
inviare EMAIL

Esempio reale di serp Google su un sito infetto:

The screenshot shows a mobile browser interface with a red header bar. The header contains a back arrow, a lock icon, the text "Phishing Warning", and the URL "https://www.google.com". On the far right of the header is a vertical ellipsis. Below the header, the main content area has a light gray background. At the top of this area, the text "Warning – phishing (web forgery) suspected" is displayed in bold black font. Below this, there is a message in regular black font: "The site you are trying to visit has been identified as a forgery, intended to trick you into disclosing financial, personal or other sensitive information." Further down, another message reads: "You can continue to http://[redacted]/wp-admin/maint/bwpghdnmnbdtrcvebn/standofinalsimpl/ibsa.php at your own risk." At the bottom of the content area, there is a link in blue text: "If you believe that this site is not actually a phishing site, you can report an incorrect warning." Below this link, the text "Advisory provided by Google" is visible.

Tools di Analisi

Alcuni tools di analisi molto utili in caso si sospetti di essere finiti in blacklist:

<http://multirbl.valli.org/>



<https://mxtoolbox.com/>



<https://www.mail-tester.com/>



Tool per verificare se un IP o dominio sia in una blacklist

<http://multirbl.valli.org/>

Non sicuro | multirbl.valli.org/lookup/unimore.it.html

Home multirbl lookup Infos about all RBLs

The complete IP check for sending Mailservers

Test IPv4/IPv6 address or domainname
[FCrDNS & DNSBL lookups] Send

DNSBL Blacklist Test Summary 54 of 54 tests done.
Results Not listed: 52 Blacklisted: 2 Brownlisted: 0 Yellowlisted: 0 Whitelisted: 0 Neutrallisted: 0 Failed: 0
Processing All done

DNSBL Combinedlist Test Summary 6 of 6 tests done.
Results Not listed: 6 Blacklisted: 0 Brownlisted: 0 Yellowlisted: 0 Whitelisted: 0 Neutrallisted: 0 Failed: 0
Processing All done

DNSBL Whitelist Test Summary 7 of 7 tests done.
Results Not listed: 7 Blacklisted: 0 Brownlisted: 0 Yellowlisted: 0 Whitelisted: 0 Neutrallisted: 0 Failed: 0
Processing All done

DNSBL Informationalist Test Summary 1 of 1 tests done.
Results Not listed: 1 Blacklisted: 0 Brownlisted: 0 Yellowlisted: 0 Whitelisted: 0 Neutrallisted: 0 Failed: 0
Processing All done

DNSBL Blacklist Test

832 unimore.it	Ospam URLBL Listings
759 unimore.it	Ospam URLBL Listings (mirror)
732 unimore.it	abuse.ch ZeuS Tracker Domain
720 unimore.it	abuse.ro URI RBL
853 unimore.it	Abusix Mail Intelligence Domain Blacklist
551 unimore.it	Blog Spam Blocklist (empty.us)
550 unimore.it	Blog Spam Blocklist (spamlookup.net)
856 unimore.it	Brukalai.it DNSBL black
857 unimore.it	Brukalai.it DNSBL light
798 unimore.it	fmb.la.bl
799 unimore.it	fmb.la.comunicando
802 unimore.it	fmb.la.nsbl

Non sicuro | rfc-clueless.org/lookup/unimore.it

RFC² Realtime List

Check a Host
Invia

Time	List	Request Type	Status	Comment
2017-05-08 14:48:32	DSN	ADD	ACCEPTED	show
2017-05-08 14:44:23	POSTMASTER	ADD	ACCEPTED	show

unimore.it IS listed in an RFC² list.

For more information please read [our listing policy](#) and review our [frequently answered questions](#).
You might be interested in [removal](#) if this domain is now properly configured.
If you send eMail from this domain, but do not manage it yourself, you may want to [contact its postmaster](#) to ask that this be fixed.
If this domain should be added to additional lists, [you may provide evidence on the listing page](#).

[RFC² Home](#)
[Other SaveRPIGeeks projects](#)

Domain shares an MX record (alt1.aspmx.l.google.com) for a mail exchange which is known to not handle mail correctly.

Tool per analisi multiple su dominio e IP

<https://mxtoolbox.com/>

The screenshot shows the MX Toolbox website's SuperTool interface. A search bar contains the domain "unimore.it". Below it, a button labeled "Blacklist Check" is followed by a dropdown menu. A large yellow starburst graphic on the right side of the page contains the text: "Fa anche un monitoraggio costante su un indirizzo IP + alert!". The main content area displays a message: "X BLACKLISTING isn't the ONLY email delivery issue". Below this, a table lists various blacklists against which the domain was checked, all of which were found to be OK. The table has two columns: "Blacklist" and "Result". The results are as follows:

Blacklist	Result
ivmURI	OK
SEM FRESH	OK
SEM URI	OK
SEM UNIRED	OK
SORBS RHSBL BADCONF	OK
SORBS RHSBL NOMAIL	OK
Spamhaus DBL	OK
SURBL multi	OK

At the bottom of the page, there is a section titled "SMTP Diagnostics" with a "Mail Server" input field and a "Test Email Server" button.



Tool per analizzare le mail (si invia una mail all'indirizzo indicato)

<https://www.mail-tester.com/>



Cosa bisogna fare?

1) Effettuare una scansione
del sito

2) Rimuovere i file infetti

3) Applicare le patch di
sicurezza

CASO 1

Rimuovendo i files malevoli e applicando le patch per impedire nuovi attacchi nell'immediato, il sito non è più compromesso.

A questo punto si segnala tramite appositi tools ai motori di ricerca ed alle singole blacklist che il sito è stato rimesso in condizioni di sicurezza.



Tempi di attesa:
da 2 a 15 giorni

Cosa bisogna fare?

1) Tutti i punti del CASO 1

2) + Cambiare indirizzo IP

The screenshot shows a web hosting control panel interface. At the top, there are navigation links: Home, Domains, and a magnifying glass icon. Below this, the title "Web Hosting Access for example.com" is displayed. A sub-header reads: "Here you can view the IP addresses associated with your subscription and change them if needed." Under this, there is a section titled "IP addresses". On the left, there is a sidebar with links: Services, Customers, Killers, and Domains (which is highlighted in blue). In the main content area, there is a table with one row. The first column is labeled "IP address" and contains three options: "10.82.82.13 (shared)", "10.82.82.13 (shared)" (which is selected and highlighted in blue), and "10.82.81.97 (shared)". An orange arrow points from the text "Cambiare indirizzo IP" in the previous slide to the "10.82.82.13 (shared)" dropdown menu.

CASO 2

A volte non è possibile aspettare così tanto per una azienda per poter ricominciare ad inviare mail ed avere il sito web attivo.

In questo caso si cambiano gli indirizzi IP del server ove possibile o in alternativa si acquista un servizio di invio SMTP per le sole email.

Si acquista un IP aggiuntivo e lo si installa nel pannello di amministrazione (nell'esempio, PLESK)

Tempi di attesa: da 1 a 2 giorni



Cosa bisogna fare?

SE NON ABBIAMO IL CONTROLLO DEI DNS

1) Tutti i punti del CASO 1

2) + Migrazione

CASO 3A

Nel caso non sia possibile un cambio di IP, si migra ad un altro servizio di hosting presso diverso provider o si cambia tipologia di servizio presso lo stesso (ad esempio da hosting a VPS).

Migrazione
Hosting Provider



Molti fornitori di hosting forniscono dei tools per la migrazione.

Bisogna anche ricreare tutte le **email** ed eventualmente **trasferire tutta la posta** nei server se richiesto, se già non su servizio esterno.

Tempi di attesa: da 1 a 15 giorni



Cosa bisogna fare?

SE ABBIAMO IL CONTROLLO DEI DNS

1) Tutti i punti del CASO 1

2) + Migrazione +
puntamento DNS

DNSSEC

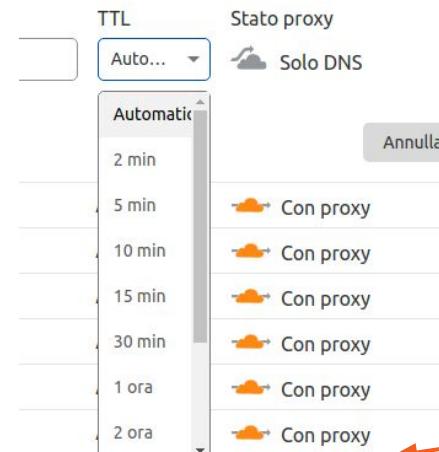
DNSSEC protegge dalle risposte DNS manomesse. Le zone protette da DNSSEC sono firmate con crittografia per garantire che i record DNS ricevuti siano identici ai record DNS pubblicati dal proprietario del dominio.

DNSSEC per il tuo dominio verrà abilitato automaticamente nelle successive 24 ore.

Disabilita DNSSEC

CASO 3B

Se abbiamo il controllo dei DNS invece, possiamo semplicemente puntare i DNS al nuovo hosting una volta che abbiamo tutto pronto e funzionante.



TTL
prima del passaggio,
abbassare il TTL per
ottenere un
passaggio
immediato.
(Nell'esempio, TTL
su **CDN** **cloudflare**)

Tempi di attesa: da 1 a 2 giorni

Usare anche DNSSEC, v=DMARC e v=spf

Propagazione

Per verificare la propagazione e dove questa sia avvenuta, ecco un utile tool che verifica lo stato della propagazione in tutto il mondo:

<https://www.whatsmydns.net/>

The screenshot shows the whatsmydns.net website. At the top, there's a search bar with 'google.it' and a dropdown menu set to 'A'. Below the search bar is a sidebar with a list of cities and their IP addresses, each followed by a green checkmark. The main content area is titled 'DNS Propagation Checker' and contains a brief description of what the service does. Below this is a small advertisement for a BEKO espresso machine. The most prominent feature is a world map where numerous green checkmarks are placed over specific locations, indicating successful propagation. A red box highlights the 'DNS Propagation Checker' title, and a red arrow points from this box to the world map.

Città / Paese	IP Address	Status
San Jose CA, United States	Corporate West	✓
Kansas City, United States	WholeSale Internet	✓
Dothan AL, United States	Comodo	✓
Miami FL, United States	AT&T	✓
New York NY, United States	Speakeasy	✓
London ON, Canada	Golden Triangle	✓
Ciudad Acuña, Mexico	Mesetaable	✓
Santa Cruz do Sul, Brazil	Claro	✓
Almería, Spain	Vodafone Ono	✓
Cambridge, United Kingdom	WCMC	✓
Lille, France	Compleat SAS	✓
Diemen, Netherlands	Tele2 Nederland	✓
Glostrup, Denmark	Sentia	✓
Leipzig, Germany	Universität Leipzig	✓
Bern, Switzerland	Swiscom AG	✓





Nota importante

Gli IP che ci vengono assegnati in fase di **acquisto** **NON SONO** per forza “CLEAN”

Quando acquistiamo un nome di dominio, o un indirizzo ip da collegare ad un servizio, nessuno ci da garanzia che questi non siano finiti in blacklist prima.





IP CLEAN

Un esempio classico è proprio sulle VPS a basso costo che abbiamo visto in precedenza.

Poiché costano poco ed è possibile acquistarle solamente per qualche mese o addirittura ad ORE, è molto probabile che questi siano stati usati per qualche attacco in precedenza e poi abbandonato il servizio :

The screenshot shows the OVHcloud website's VPS pricing page. It features four plan cards:

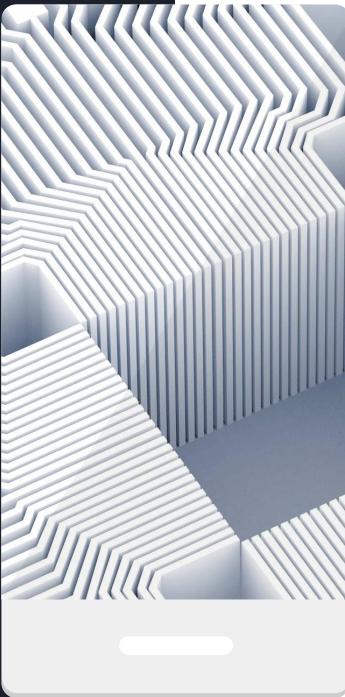
- VALUE**: 4,60 € + IVA/mese (cioè 5,61 € IVA incl./mese). Includes 1 vCore, 2 GB, 40 GB SSD NVMe, and 250 Mbps illimitato*. Call-to-action: [Ordina adesso](#).
- ESSENTIAL**: 9,20 € + IVA/mese (cioè 11,22 € IVA incl./mese). Includes 2 vCore, 4 GB, 80 GB SSD NVMe, and 500 Mbps illimitato*. Call-to-action: [Ordina adesso](#).
- COMFORT**: 18,40 € + IVA/mese (cioè 22,45 € IVA incl./mese). Includes 4 vCore, 8 GB, 160 GB SSD NVMe, and 1 Gbps illimitato*. Call-to-action: [Ordina adesso](#).
- ELITE**: A partire da 39 € + IVA/mese (cioè 33,67 € IVA incl./mese). Includes 8 vCore, 8 GB, 640 GB SSD NVMe, and 2 Gbps illimitato*. Call-to-action: [Scopri di più →](#).

L'indirizzo IP è stato compromesso, e andrà al prossimo acquirente!



Verificare in fase di startup

Quando si acquista un nuovo Dominio,
sarebbe meglio verificare subito se il suo IP sia finito in blacklist.



In caso di IP condiviso
(esempio: hosting economici)

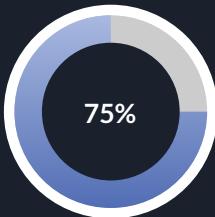
questo rischio è sempre dietro l'angolo perché è sufficiente che uno dei siti che condividono l'IP sia vulnerabile per causare problemi a tutti gli altri.

Spesso si consiglia l'acquisto di IP dedicati anche in caso di hosting economici.

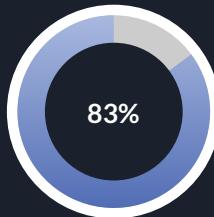


Consigli sulla sicurezza

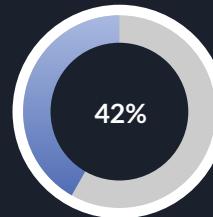
Quattro utili consigli:



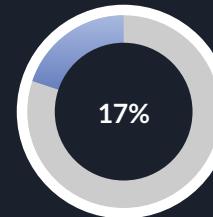
Tenere separate Mail server e Web Server



Evitare l'uso scorretto di CMS



Scansione continua sui files del server e sulle vulnerabilità del server stesso.



Installazione costante delle Patch di vulnerabilità

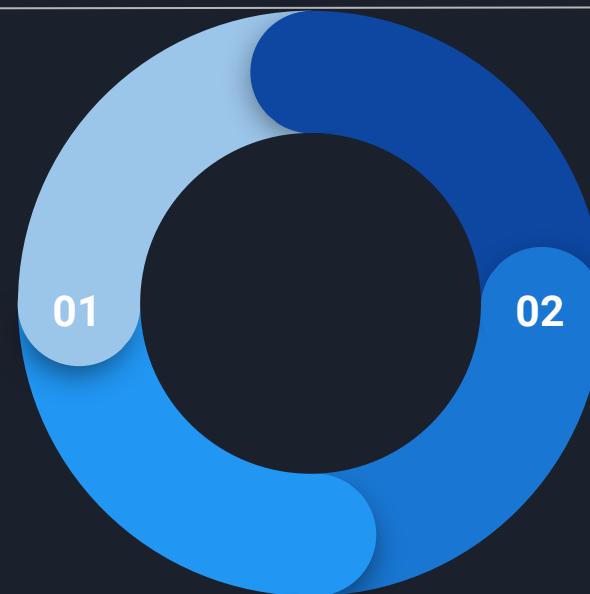




Più importante di tutto il resto

Backup

Resta di vitale importanza un corretto uso dei backup, con la frequenza giusta per le esigenze del sito web stesso (orario, giornaliero..)



Backup Remoto

La repository di destinazione deve essere ESTERNA al server dove risiede il sito di produzione, possibilmente su un **diverso fornitore**.

RIEPILOGANDO

La SALUTE di un indirizzo IP è importante e va monitorata.

Se il sito è compromesso, può essere un problema dei files del sito oppure del web server.

In entrambi i casi l'IP ne può venire danneggiato creando disservizi importanti.

Consigli

Evitare i CMS ma preferire uno sviluppo custom o con framework

Usare servizi Saas

Differenziare Mail server da Web Server

Monitoraggio costante degli indirizzi IP (MX toolbox)

Verifica iniziale

Scansioni continue sui files

Aggiornamento costante delle patch sul web sever

Aggiornamento costante delle patch sul CMS