

Per questo progetto ho scelto di effettuare l'OSINT su Forno Brisa, una panetteria specifica di Bologna, una bella start-up del territorio.

Scrivi Il Sole 24 Ore:

Nata nel 2015 a Bologna, sulle ceneri di un ex-forno di quartiere, Forno Brisa è l'idea di quattro ragazzi, capitanati da Pasquale Polito, che decidono di cambiare vita, dedicarsi all'arte della panificazione e sovvertire l'immagine tradizionale del fornaio.

Diventata in breve punto di riferimento per pane, pizze, dolci da forno compresi i lievitati delle feste, oggi l'azienda conta 39 persone di cui 20 donne e 19 uomini (con un'età media sotto i 30 anni).

[...]

Quattro i punti vendita in città e un fatturato 2021 che si è chiuso superando i 2 milioni di euro, ma che – dicono – è in crescita: si aspettano di centrare l'obiettivo 3 milioni per il 2022. Il 49% del pane sfornato proviene dalle farine prodotte in biologico in un'azienda agricola di proprietà in Abruzzo e da campi in filiera diretta.

Il primo step è stato effettuare una ricerca avanzata tramite l'**Advanced Image Search** di Google per trovare più dipendenti possibili, soprattutto quelli di alto livello:

Advanced Image Search

Find images with...

all these words:

this exact word or phrase:

any of these words:

none of these words:

To do this in the search box.

Type the important words: winter hour/frost

Put exact words in quotes: "Frost Flower"

Type OR between all the words you want: trees OR woods OR grasses

Put a minus sign just before words that you don't want: -linkedin

Then narrow your results by...

image size:

any aspect ratio:

colours in the image: ☒ any colour ☐ full colour ☐ black & white ☐ transparent ☐ this colour

type of image:

region:

site or domain:

file type:

usage rights:

Advanced Search

LinkedIn Chiara Parisi - Bakery Chef - Forno ...

LinkedIn Pasquale Polito - General Manager ...

LinkedIn Pasquale Polito - General ...

LinkedIn Il Forno di Calzolari | LinkedIn

FORNO BRISA & Friends MANCANO SOLO 3 GIORNI ALLA FINE DELLA CAMPAGNA DIVENTA ANCHE TU UN NOSTRO SOCO SU: MAMA...

LinkedIn Pasquale Polito - Gener...

The Creative Brothers Forno Brisa, i panificatori ...

LinkedIn La Brisnonna | LinkedIn

LinkedIn La Brisnonna | Link...

FORNO BRISA & Friends MANCANO SOLO 7 GIORNI ALLA FINE DELLA CAMPAGNA PRIMA CHE SIA TROPPO TARDE!

LinkedIn Pasquale Polito - Genera...

LinkedIn Lorenzo Zucchi - Resp...

Agencfood Forno Brisa lancia il...

LinkedIn Alice Bergomi - Marketin...

LinkedIn Lucio Fusco - Store ...

CiboToday dello spaccio del Forno B...

LinkedIn Clementina Verrocchio - ...

Horeca News Forno Brisa presenta il Veganone, il ...

Horecanews.it Forno Brisa festeggia con la s...

Il Sole 24 ORE Forno Brisa, crowdfunding a quota 3,5 ...

La Gazzetta del Gusto Forno Brisa di Bologna: cronaca ...

Il Fatto Alimentare Ricette Rubate, il libro del Forno ...

LinkedIn La Brisnonna | LinkedIn

Individuo in particolare Pasquale Polito, già menzionato nell'articolo de Il Sole 24 ore, che da LinkedIn risulta essere General manager dell'azienda. Con **Webmii** approfondisco la sua figura:

The screenshot shows the Webmii profile of Pasquale Polito. At the top, there's a search bar and the Webmii logo. Below the name 'Pasquale Polito' is a blue box with a '4.17' Webmii score. To the right is a profile picture. Below the name, it says 'General Manager' and 'Forno Brisa'. There are links to the App Store and a 'Share 0' button. Below this, there's a list of contacts including Emilia Romagna, Davide Sarti, Elisa Vian, Con Pasquale, Don Pasquale, Pietro Monti, Damien Stretch, Jack Lewery, Alex Giustolisi, Andrea Michinelli, Salvatore Viola, Cristina Caroli, Robin Marastoni, Natalia Rossi, Pasquale Barberio, and Pasquale Cell. Below the contacts, there are two posts. The first post is from 'NSW Touch Football' and the second is from 'Andrea Michinelli'.

Il primo nome e cognome nei contatti è Davide Sarti, che scopro essere socio e co-fondatore insieme a Pasquale.

Sempre tramite Google riesco a trovare il profilo Instagram di Pasquale (profilo aperto), mentre purtroppo non riesco a reperire quello di Davide.

https://www.instagram.com/pasquale_polito_/?hl=en

The screenshot shows the Instagram profile of Pasquale Polito. At the top, there's the Instagram logo and 'Log In' and 'Sign Up' buttons. Below the logo is a profile picture of a dog. To the right of the profile picture, it says 'pasquale_polito_' and 'Follow'. Below the name, it says '225 posts', '1,665 followers', and '2,643 following'. Below this, it says 'Pasquale Polito', '@fornobrisa', and 'www.fornobrisa.it'. Below the profile information, there are two tabs: 'POSTS' and 'TAGGED'. Below the tabs, there are three post thumbnails: a close-up of a dog's face, a bright light, and a dog's head.

A questo punto mi concentro sul sito, www.fornobrisa.it.

WHOIS

WHOIS è un protocollo di interrogazione utilizzato per ottenere informazioni sui registranti di nomi di dominio, come proprietari, contatti tecnici e dettagli del registrar. In pratica, consente di identificare

chi possiede un dominio o un indirizzo IP specifico. Le informazioni raccolte tramite WHOIS sono utilizzate per vari scopi, tra cui la gestione dei domini, la sicurezza e la risoluzione di problemi legati all'identificazione online. Tuttavia, nel corso degli anni, sono emerse preoccupazioni sulla privacy, portando a limitazioni e regolamentazioni nell'accesso ai dati WHOIS per proteggere le informazioni personali.

```
kali@kali: ~  
File Actions Edit View Help  
$ whois fornobrisa.it  
*****  
* Please note that the following result could be a subgroup of *  
* the data contained in the database. *  
* *  
* Additional information can be visualized at: *  
* http://web-whois.nic.it *  
*****  
Domain: fornobrisa.it  
Status: ok  
Signed: no  
Created: 2015-09-09 18:42:40  
Last Update: 2023-09-25 00:48:38  
Expire Date: 2024-09-09  
Registrant  
Organization: Breaders srl  
Address: via galliera 34/d,  
bologna  
40121  
BO  
IT  
Created: 2019-08-01 13:13:28  
Last Update: 2019-08-01 13:13:28  
Admin Contact  
Name: davide sarti  
Organization: Breaders srl  
Address: via galliera 34/d,  
bologna  
40121  
BO  
IT  
Created: 2019-08-01 13:13:28  
Last Update: 2019-08-01 13:13:28  
Technical Contacts  
Name: davide sarti  
Organization: Breaders srl  
Address: via galliera 34/d,  
bologna  
40121  
BO  
IT  
Created: 2019-08-01 13:13:28  
Last Update: 2019-08-01 13:13:28  
Registrar  
Organization: 1 Api GmbH  
Name: 1API-REG  
Web: http://www.1api.net  
DNSSEC: yes  
Nameservers  
ns81.domaincontrol.com  
ns82.domaincontrol.com
```

Anche nell'output di Whois compare il nome di Davide Sarti, ma non c'è purtroppo nessun contatto (mail o telefono).

Scopriamo che il dominio è in scadenza il 9/09/24 ed è registrato tramite www.1api.net: queste informazioni potrebbero essere utilizzate da malintenzionati per simulare problemi con la registrazione o il rinnovo della stessa, in un tentativo di phishing.

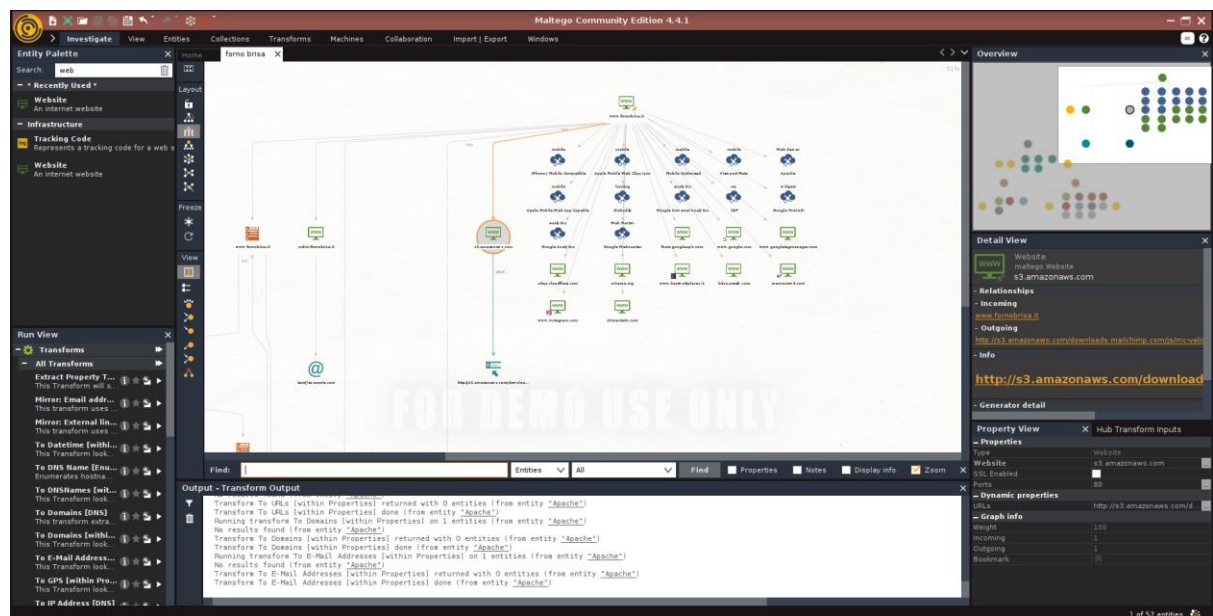
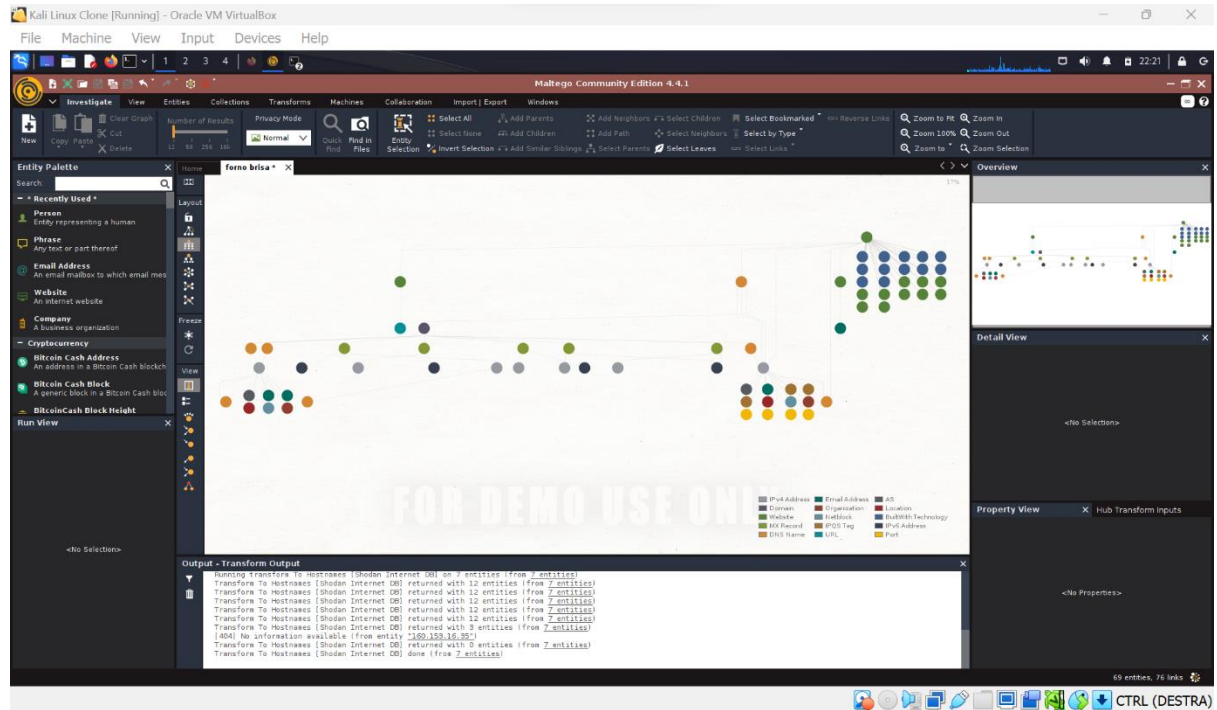
È inoltre presente l'informazione DNSSEC: yes.

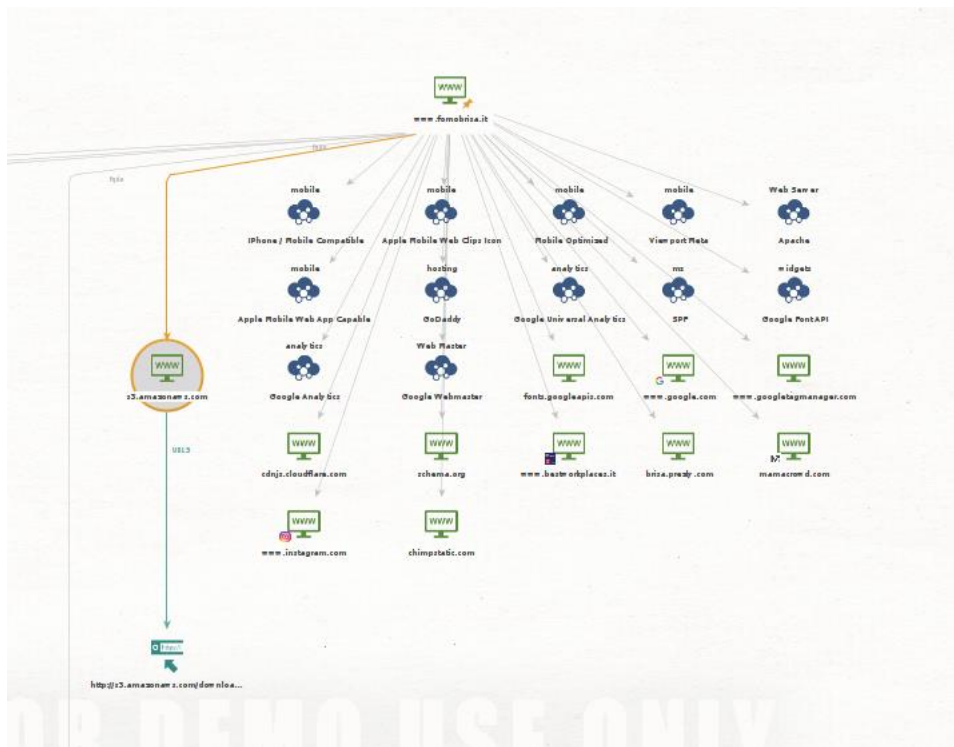
DNSSEC è un'estensione del sistema DNS che garantisce autenticità e integrità delle informazioni DNS. Nel contesto WHOIS, indicare DNSSEC per un dominio significa che quel dominio utilizza misure di sicurezza per prevenire manipolazioni o falsificazioni dei suoi record DNS. Essenzialmente, è un meccanismo di sicurezza per rafforzare la validità delle informazioni associate a un dominio.

MALTEGO

A questo punto creiamo un nuovo schema su **Maltego**. Il nostro nodo zero sarà proprio www.fornobrisa.it.

Dopo vari transform, lo schema risulterà come segue. Vediamo le sue parti nel dettaglio.



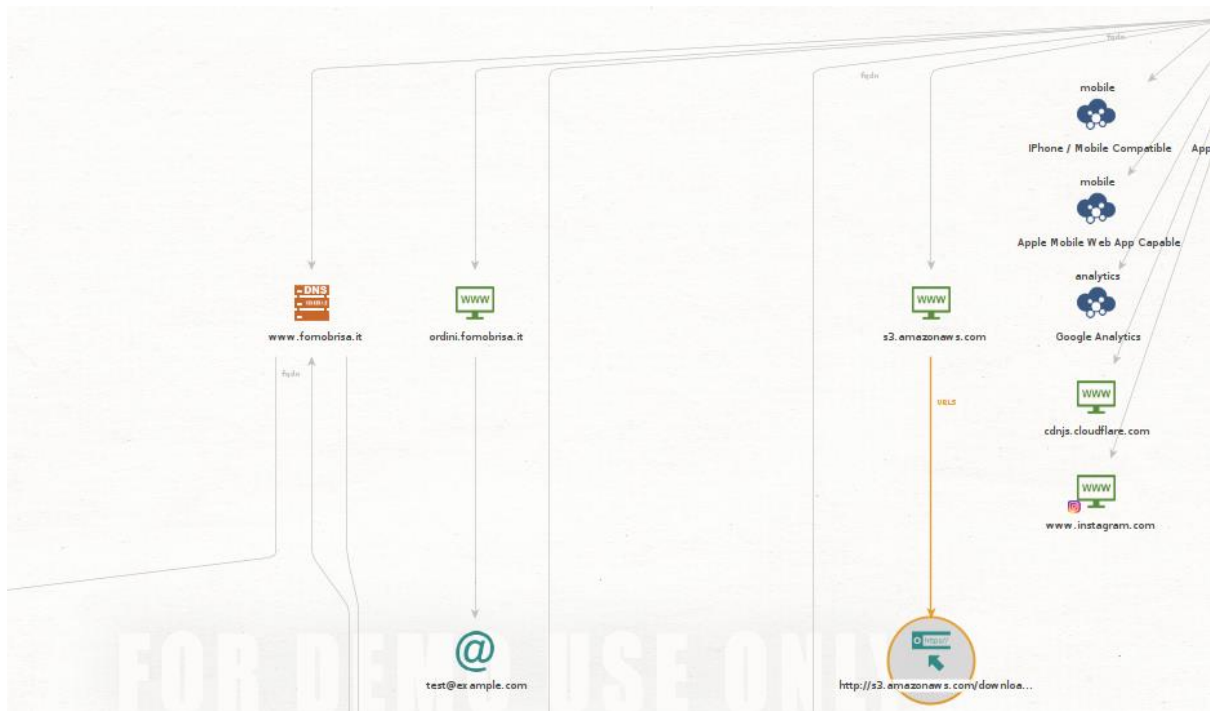


Tramite il trasformatore Built With, scopriamo le diverse tecnologie con cui è stato creato il sito. Fra gli elementi più interessanti spiccano:

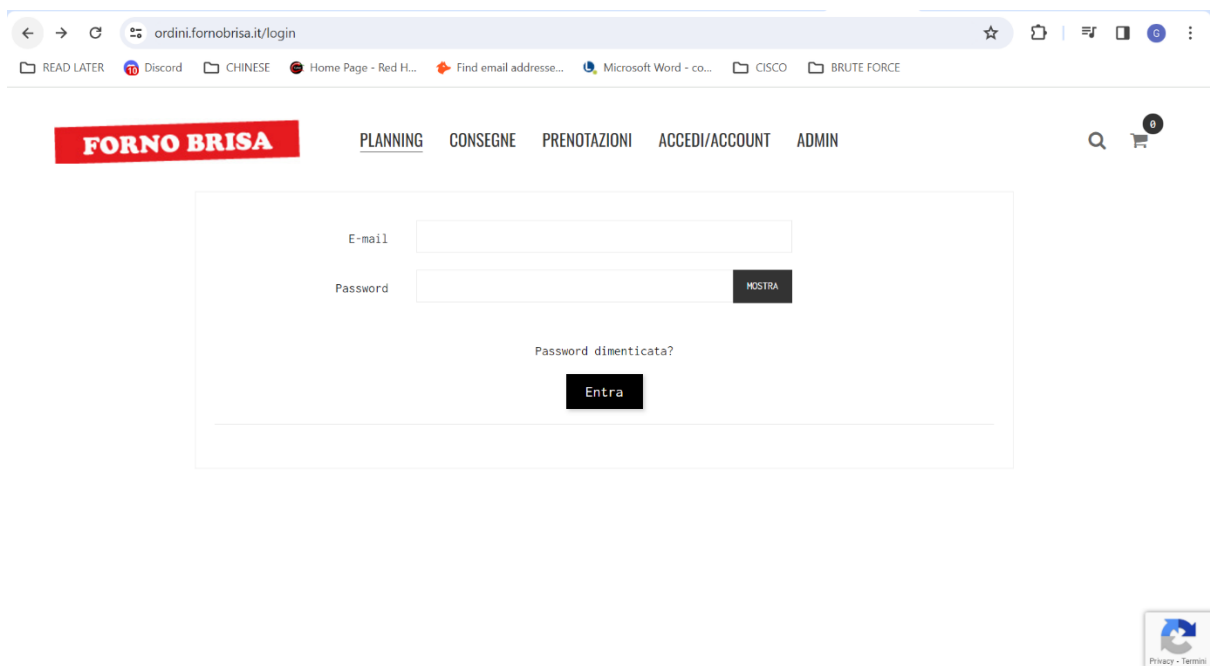
- Il Web Server è Apache. Apache è un popolare server web open-source utilizzato per ospitare siti web. Fornisce la capacità di servire pagine web su Internet, gestire richieste HTTP e supportare linguaggi di programmazione come PHP e Perl;
- L'hosting è di GoDaddy;
- Viene utilizzato il record SPF per verificare l'autenticità e la provenienza delle email, riducendo il rischio di email fraudolente o spam.

Se invece approfondiamo i link esterni, emerge chimpstatic che è legato a Mailchimp. Da cui deduciamo che è in uso Mailchimp, piattaforma leader per il marketing via email, specialmente utilizzata da piccole e medie imprese. Molto interessante anche il link a s3.amazonaws.com: Amazon S3 è un servizio di archiviazione cloud di Amazon Web Services (AWS). "s3.amazonaws.com" è l'indirizzo per accedere ai dati archiviati su S3, dove i dati vengono conservati in "bucket" virtuali.

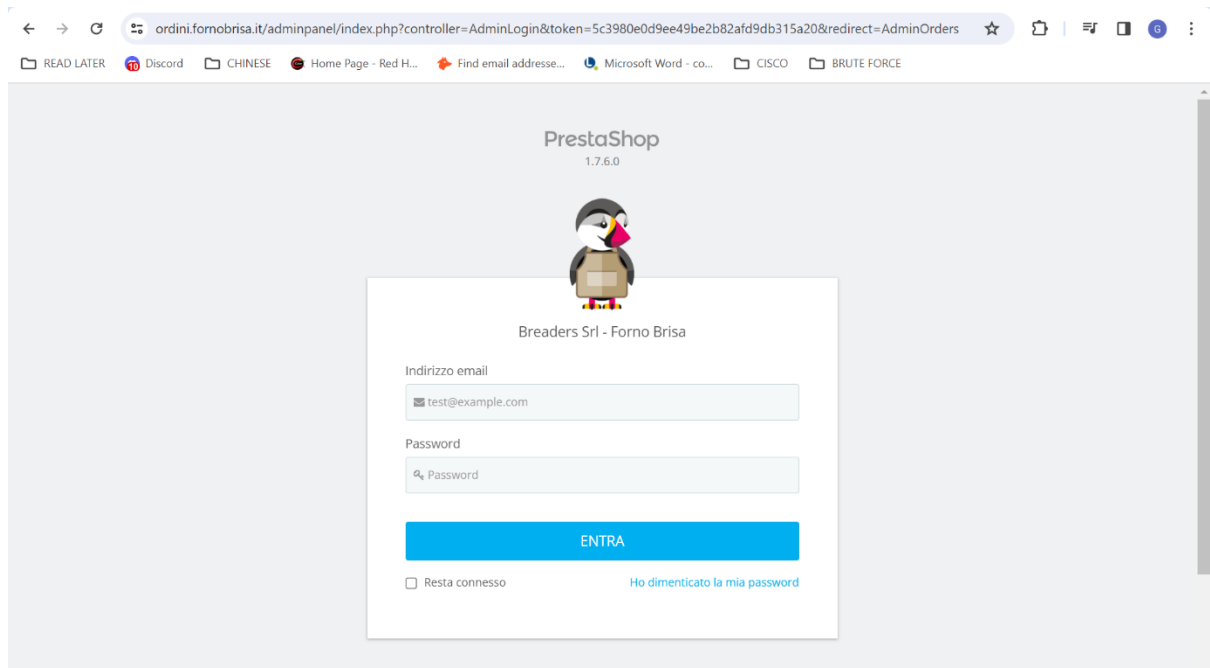
Spostandoci verso sinistra nello schema, troviamo un altro indirizzo: ordini.fornobrisa.it.



Lo visitiamo e sembra proprio un sito che non dovrebbe essere visibile o accessibile al pubblico:



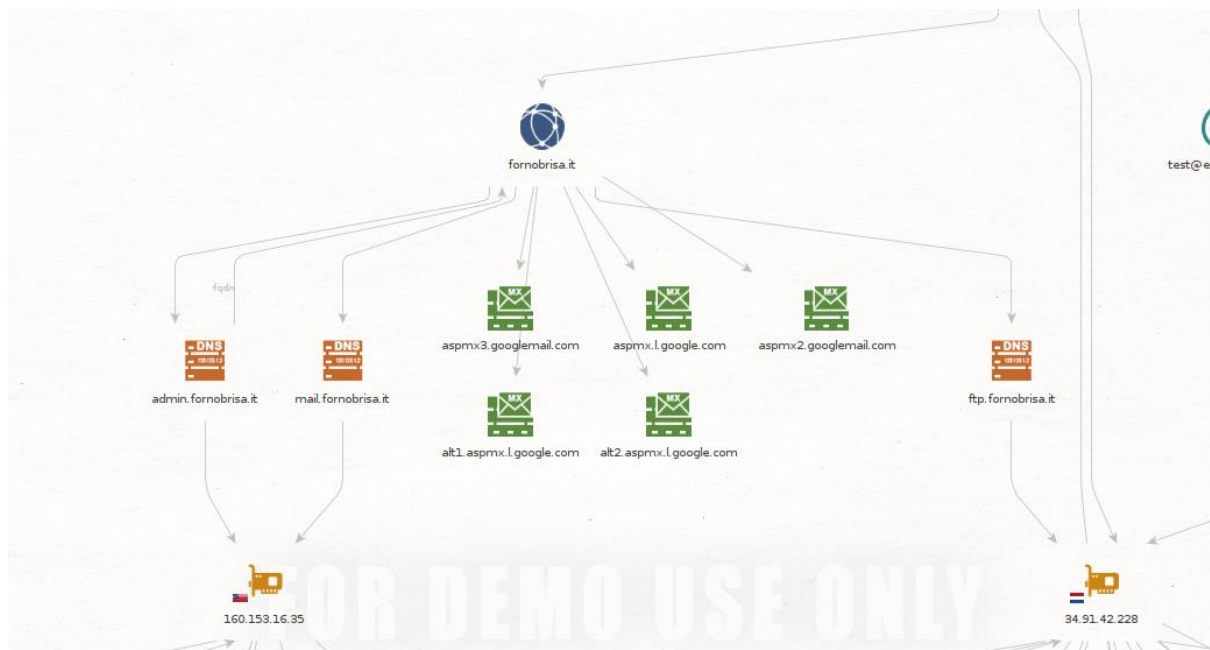
Di particolare interesse la tab ADMIN, che rimanda ad una finestra di login PrestaShop:



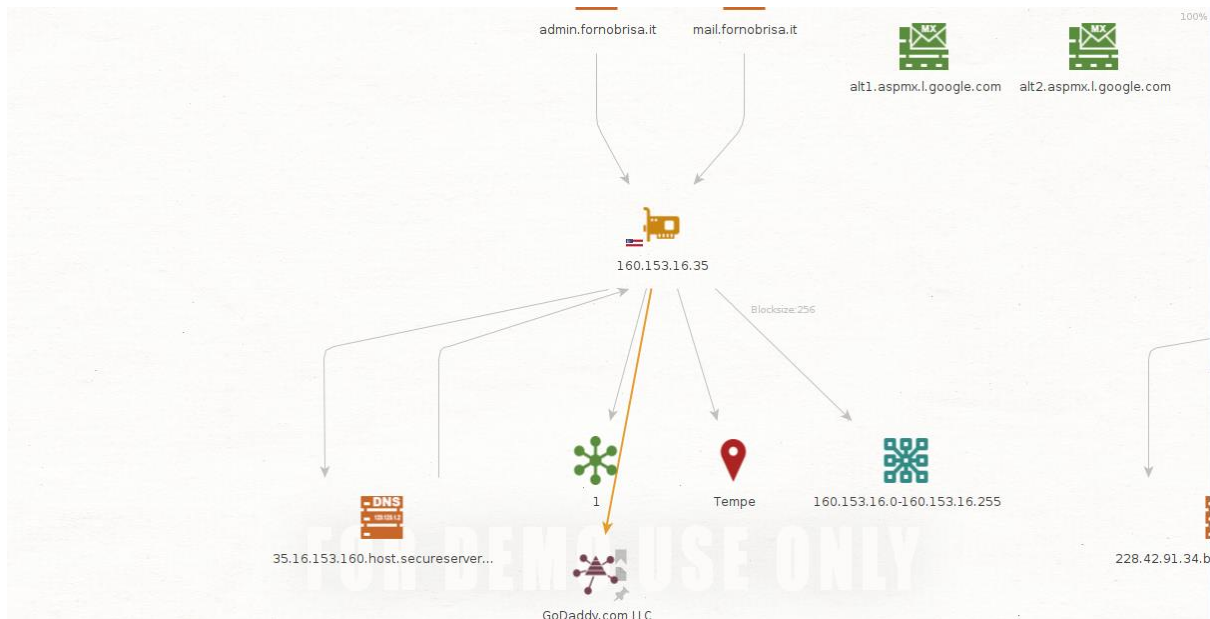
PrestaShop è una piattaforma open-source per e-commerce. Permette di creare negozi online personalizzati, gestire prodotti, ordini, pagamenti e altri aspetti del commercio elettronico.

Questa tab potrebbe prestarsi ad attacchi Brute Force, se non adeguatamente protetta.

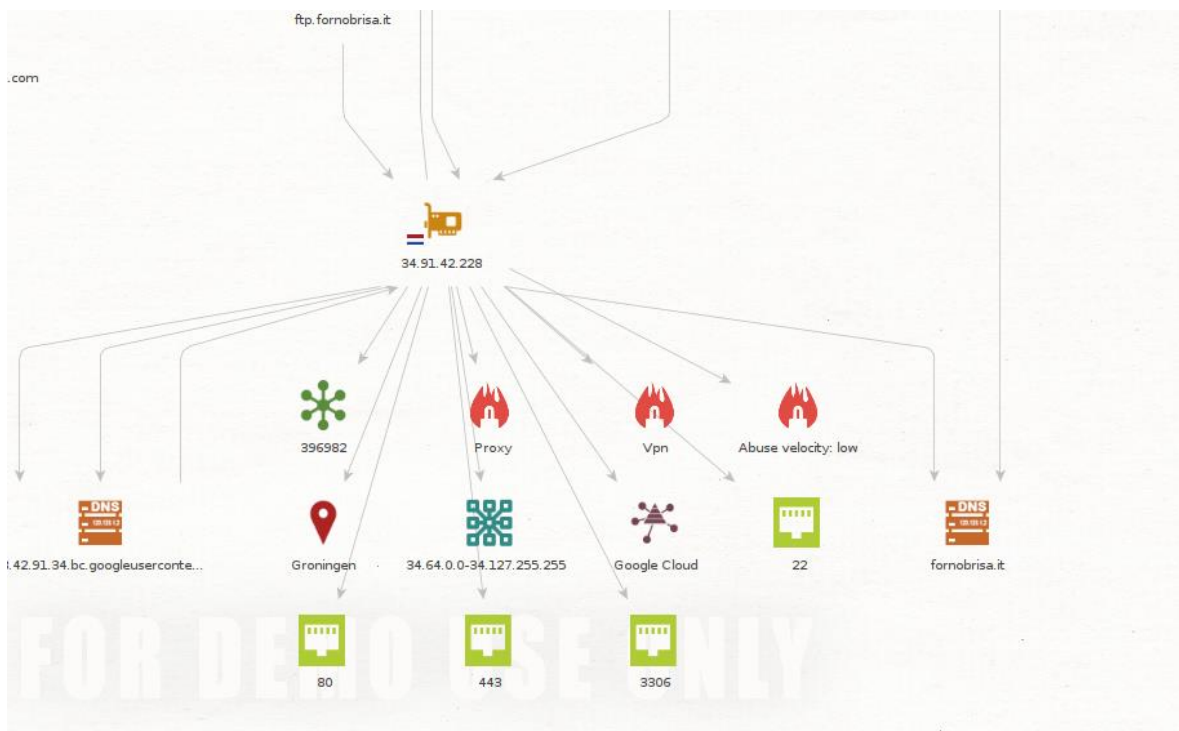
Spostandoci a sinistra nello schema di Maltego, dal dominio `fornobrisa.it` riusciamo a ricavare ben 3 DNS: `admin.fornobrisa.it` e `mail.fornobrisa.it` e `ftp.fornobrisa.it`:



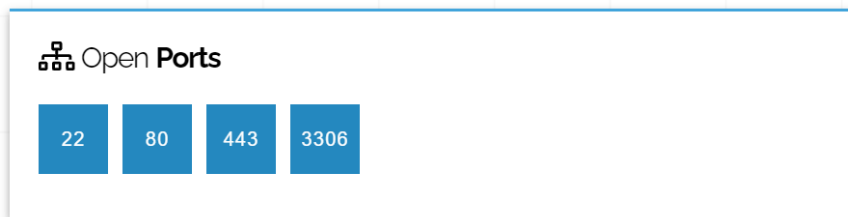
I primi due sono collegati ad un IP che, a parte essere collegato ad un netblock (blocco di indirizzi IP consecutivi in una particolare rete), non offre spunti particolarmente interessanti. Interrogato su questo indirizzo, **Shodan** non dà alcun risultato.



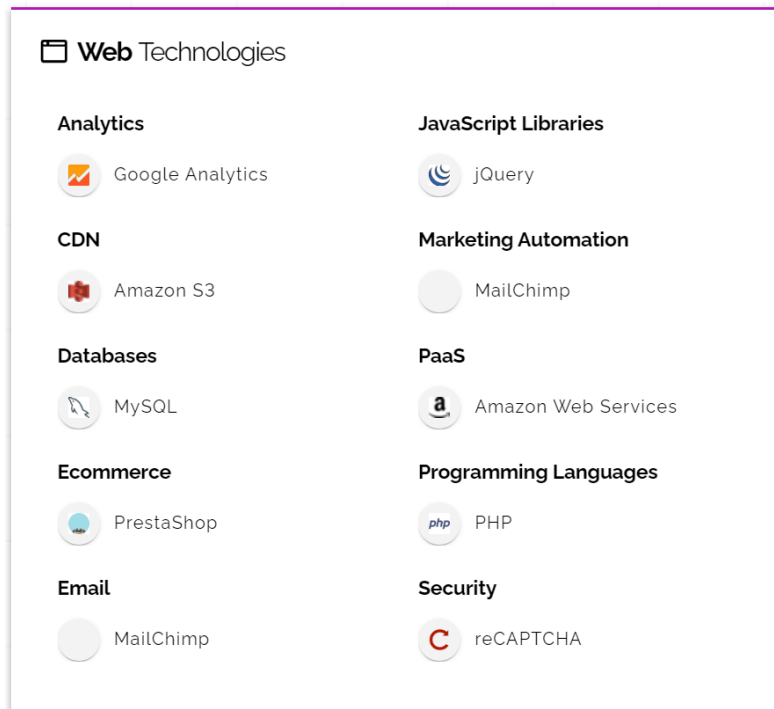
L'IP legato a ftp.fornobrisa.it, invece, oltre al proxy e alla VPN presenta 4 porte che andiamo ad approfondire con **Shodan**.



Da **Shodan**:



Troviamo riconfermate inoltre le informazioni già reperite prima:



Sulla porta 22, troviamo il servizio SSH. SSH è un protocollo crittografico utilizzato per l'accesso sicuro a server e dispositivi remoti su una rete.

Configurando e permettendo l'accesso SSH su una porta (la porta 22 è quella standard), gli amministratori di sistema possono connettersi in modo sicuro al server per gestire, configurare o eseguire operazioni sul sistema remoto utilizzando comandi SSH. Tuttavia, è essenziale mantenere la sicurezza configurando correttamente SSH, come disabilitando l'accesso root remoto, utilizzando autenticazione a due fattori e limitando l'accesso solo a indirizzi IP autorizzati, per proteggere il server da potenziali minacce o attacchi.

```
// 22 / TCP | 273071694 | 2023-12-18T17:22:08.722537

OpenSSH 7.4p1 Debian 10+deb9u7

SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDf3vBYCT1Lnz2Sa56jdhW4wpUVQeAENYxOTEPXvUTr12
8zJGD3bydwT0Qu+FvP0nOCXIVjaLhgeySM8V+L7Th018/6S+Xyu17coMY3XLUmhdaz0RegtAQIyR
iuq1Rd7QRBo32DgnRHgMSaY86/SOK1uhWnp/dGwQGFRIUDCY30/SfcQsQgy+Du/b24oM4Vd15p3W
92H38FVJcRWH05JnphFEDF4FQ6tCYVRsz2+uH5GIAVpVArnhMYL8nK9Wcb/H43+3uSC1dhTFLcNt6
dzoAmqQbAwS1rw2AFVUGwUZrX++zYxOmZmYmwEP+sJgt9M1EaT4whC9o9T5piRrx+tzJ
Fingerprint: 34:9c:df:34:9d:89:a7:12:a6:af:95:38:e1:88:18:a3

Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256
diffie-hellman-group14-sha1

Server Host Key Algorithms:
ssh-rsa
rsa-sha2-512
rsa-sha2-256
ecdsa-sha2-nistp256
ssh-ed25519

Encryption Algorithms:
```

La porta 80 è la porta standard per il traffico HTTP non cifrato. La porta 443 è la porta standard per il traffico HTTPS, che è HTTP cifrato con SSL/TLS per garantire la sicurezza delle comunicazioni. Apache HTTP Server è uno dei server web più popolari e utilizzati al mondo. Configurando Apache per ascoltare su queste porte, il server è pronto a gestire richieste web non cifrate (porta 80) e richieste web cifrate (porta 443) per fornire contenuti web agli utenti attraverso protocolli HTTP o HTTPS, rispettivamente.

```
// 80 / TCP | -373103698 | 2023-12-21T15:52:15.357194

Apache httpd

HTTP/1.0 302 Found
Date: Thu, 21 Dec 2023 15:52:15 GMT
Server: Apache
Location: https://www.fornobrisa.it/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

Apache httpd

```
HTTP/1.1 200 OK
Date: Thu, 21 Dec 2023 11:09:08 GMT
Server: Apache
Vary: Host,Accept-Encoding
Set-Cookie: PHPSESSID=6c0b3j115vt2ta5sbnbohqa3cc; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PrestaShop-e1172269c6ca093b7c65fc5d83f99d94=def50200bacfab91e47bfe1deb5f5eb97c95a47004c7b8a77bd5a3f3bd905b684c81f95f7627be65cd214cbd87e493b34821c184ccde7d585c716722bf032e74a9b12774dc5f0c6379ee95fe19623a800363904d3413d0642f7ade989426735de2253d49243363c873997d309c82d6186e358ea060187774b18055051e493291d654256c8b37e62cfebb7c044afed3ac5ea5b74856ed4d49492001b37b722276b391ec4c479b24de7e623d60f2e21f9e12e1c5e49689280058034fb31be7b9e5c90d1949708a57bebbf255b3c54bda56f48c90dde6b23db3ff2fc0a68456b023e19acedf90d8bad09c9f7; expires=Thu, 28-Dec-2023 11:09:08 GMT; Max-Age=604799; path=/; domain=www.fornobrisa.it; secure; HttpOnly
Set-Cookie: PrestaShop-e1172269c6ca093b7c65fc5d83f99d94=def50200a9704b04158646284450667bb8f010cca5915d1a2f4cddb968e9f450e7f2d72da65f89f41011ca68c820b177a925e83f09b93c61505a0940b571b10196bd174c2a0af0844b1b5f22e1497d0956e73a8c90b741808990b1734921a821040e618fe6aeb43b6fbee13c0f19659fd9b88b7e260259d6836a1a13d2f716e9c7a02a4649f61c27e5fc47e6b8bfe16d4e9212235eb845463746c0593775d3813e1c3a3125ee57de1016076024bb321c905dd8c5471b08b2e21d58a327d0575890490f1736df799ce70a25fff10577c3523f91fd17abc0199df3965943a2b5f6ebe4978dbe73c29c6c50a3b2e5db1ca308ee3db163826f97dad5455c64c1de69964c984a4414687592397da08d0732af5bdf938a; expires=Thu, 28-Dec-2023 11:09:08 GMT; Max-Age=604799; path=/; domain=www.fornobrisa.it; secure; HttpOnly
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

SSL Certificate

Sulla porta 3306, infine, è in esecuzione MySQL, un popolare sistema di gestione di database. Se MySQL sulla porta 3306 è configurato in modo errato o non sicuro potrebbe essere esposto a tentativi di accesso:

MySQL 5.7.27-log

```
MySQL:
  Protocol Version: 10
  Version: 5.7.27-log
  Capabilities: 65535
  Server Language: 8
  Server Status: 2
  Extended Server Capabilities: 49663
  Authentication Plugin: mysql_native_password
```

Arrivata a questo punto, non ho però ancora nessun contatto mail o cellulare (ho solo il numero fisso di Forno Brisa). Dopo una lunga ricerca riesco a reperire questo indirizzo mail sul sito:

SEND

▼ Do you want to become part of our team?
write to info@fornobrisa.it

▼ Any problem with orders or shipments?
Fill the Form

▼ Do you have a cafe and want our coffee?

Great!
Great choice!

Privacy Policy

Come immaginavo, la mail è @fornobrisa.it. Quando provo però a lanciare questo dominio su **theHarvester**, non ottengo alcun risultato:

```
kali@kali: ~  
File Actions Edit View Help  
$ theHarvester -d info@fornobrisa.it  
*****  
* theHarvester 4.4.4  
* Coded by Christian Martorella  
* Edge-Security Research  
* cmartorella@edge-security.com  
*  
*****  
[*] No IPs found.  
[*] No emails found.  
[*] No hosts found.
```

Nonostante numerose ricerche e approfondimenti, non ho trovato alcuna informazione su indirizzi mail dell'azienda. L'informazione potrebbe essere ben protetta oppure posso supporre che i fondatori utilizzino una mail che non termina in @fornobrisa.it, essendo comunque l'azienda ancora piccola e non avendo dei veri e propri reparti interni.