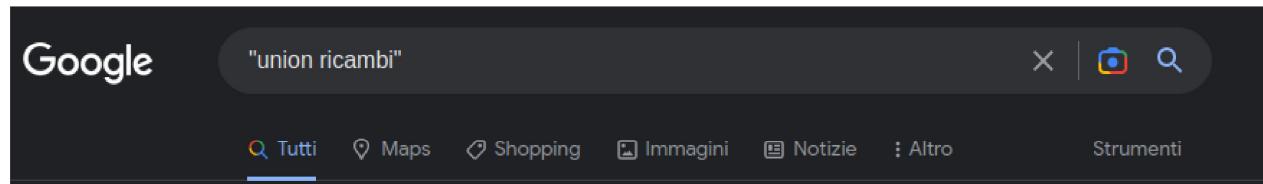
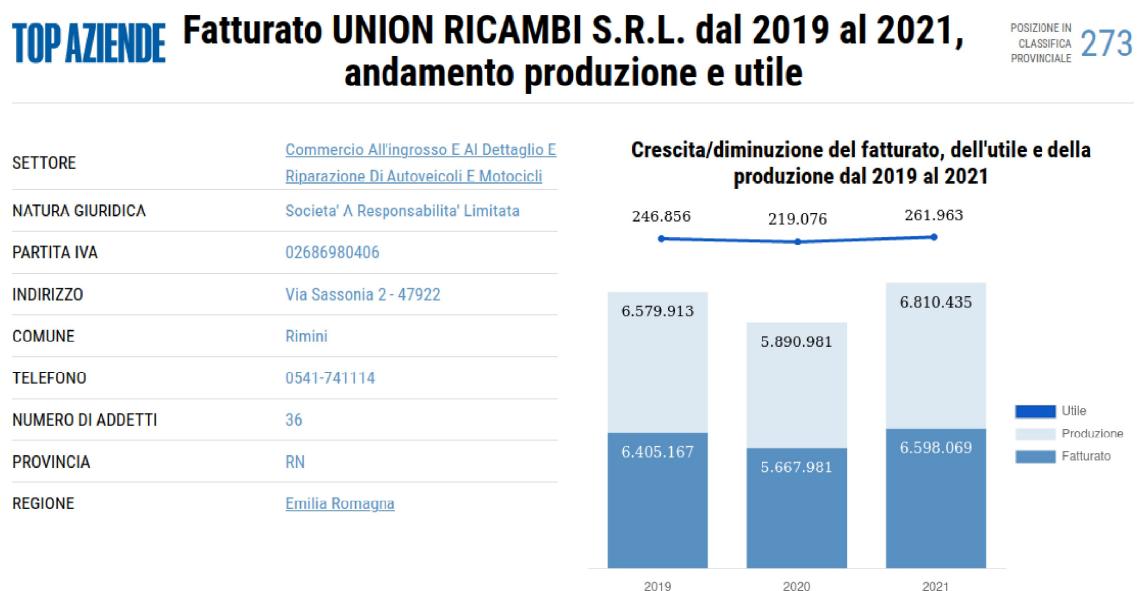


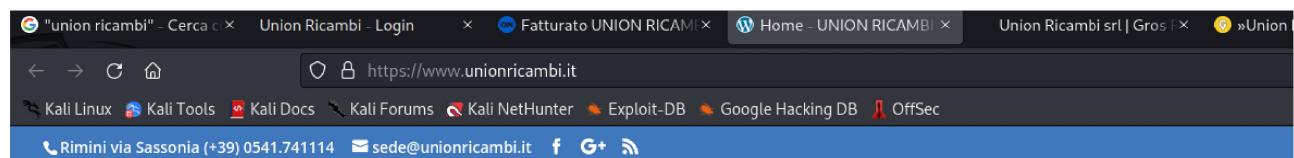
Target :UNION RICAMBI



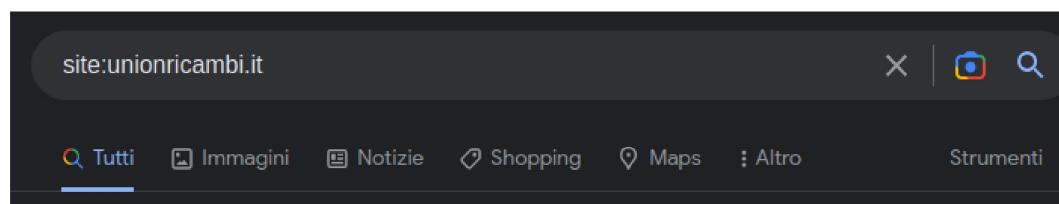
Un paio di pagine interessanti a riguardo:



Qui vediamo fatturato e numero di dipendenti



Qui notiamo che il sito è fatto con wordpress (icona in alto), inoltre possiamo già trovare una mail pubblica e il numero di telefono di una sede



Ricerca per trovare eventuali sottodomini, ma non ne trovo.

Spulciando nelle sezioni del sito troviamo un portale di login, su un altro dominio



Possiamo inoltre vedere che utilizza index.php, sarebbe possibile testare vari metodi di penetrazione.

Provo a cercare con questa query

site:blusys.it

<https://www.blusys.it> ::
Blusys Srl - Soluzioni innovative per il tuo business
Gestionali ERP. Ottimizzare le risorse, risparmiare tempo e denaro. Con Mistral tutto questo è possibile.

<https://materinddev.blusys.it> ::
Materind Srl | Il tuo partner di fiducia nelle forniture industriali
Azienda specializzata nel settore industriale; siamo rivenditori di materiali per impianti chimici, farmaceutici e trattamento vapore: valvole, ...

<https://materinddev.blusys.it/tubi> ::
TUBI - Materind Srl
Acciaio al Carbonio e leghe; Acciaio Inox e Leghe; PVC-Moplen-Rilsan-Polietilene; Rame.
Materind Srl. Via Umberto I, 36 24050 Bariano (BG). Servizio Clienti.

<https://materinddev.blusys.it/tubi/rame> ::
Rame | Materind Srl
Codice, Descrizione, Scheda tecnica. 00035260. TUBO RAME RIV.PVC 1/4. 00723222. TUBO RAME CRUDO 12X8. 02693977. TUBO RAME COTTO D.18. 03871283.

<https://coran.blusys.it> ::
b2b.blusys.it
b2b.blusys.it.

<https://union.blusys.it> ::
b2b.blusys.it
b2b.blusys.it.

Intuiamo che è un'azienda che offre servizi cloud per imprese

Blusys Srl - Soluzioni inno X union.blusys.it/admin.php X +

https://www.blusys.it/index.html

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

blusys
business solutions

HOME CONTATTI AREA RISERVATA ASSISTENZA

MISTRAL

Il gestionale intelligente che trova soluzioni *smart*

Mistral è un software completo per gestire il vostro business.

Con questo ERP integrato, la vostra azienda commerciale offrirà ai propri collaboratori lo strumento più completo per preparare offerte, perfezionare ordini, pianificare l'ottimizzazione delle scorte, vendere su piattaforme e-commerce integrate, fatturare, contabilizzare e occuparsi della parte finanziaria.

Tool kali:

Dmitry:

```
(alessio㉿kali)-[~]
$ dmitry www.unionricambi.it
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:95.110.164.90
HostName:www.unionricambi.it

Gathered Inet-whois information for 95.110.164.90
-----
inetnum:          95.110.160.0 - 95.110.167.255
netname:          ARUBA-NET
descr:            Aruba S.p.A. - Cloud Services Farm2
country:          IT
admin-c:          SS936-RIPE
tech-c:           AN3450-RIPE
status:           ASSIGNED PA
remarks:          INFRA-AW
mnt-by:           ARUBA-MNT
created:          2011-04-25T14:21:29Z
last-modified:    2012-01-29T17:28:38Z
source:           RIPE
```

```
Gathered Inic-whois information for unionricambi.it
Azione E-commerce Eventi Contatti
unionricambi.it
Status: ok
Signed: no
Created: 2009-01-14 13:29:40
Last Update: 2023-01-30 01:05:19
Expire Date: 2024-01-14

Registrant
Organization: Union Ricambi S.r.l.

Admin Contact
Name: hidden
Organization: hidden

Technical Contacts
Name: Movient srl
Organization: Movient srl
Address: Via Savelli, 72
          Padova
          35129

PD
IT
Created: 2010-06-07 16:46:25
Last Update: 2015-01-27 12:55:11

Registrar
Organization: Movient s.r.l.
Name: MOVIENT-REG
Web: https://www.mvmnet.com
DNSSEC: no

Gathered Netcraft information for www.unionricambi.it
```

Retrieving Netcraft.com information for www.unionricambi.it
Netcraft.com Information gathered

Gathered Subdomain information for unionricambi.it

```
Gathered Netcraft information for www.unionricambi.it
_____
Retrieving Netcraft.com information for www.unionricambi.it
Netcraft.com Information gathered
_____
Gathered Subdomain information for unionricambi.it
_____
Searching Google.com:80 ...
HostName:www.unionricambi.it
HostIP:95.110.164.90
Searching Altavista.com:80 ...
Found 1 possible subdomain(s) for host unionricambi.it, Searched 0 pages containing 0 results

Gathered E-Mail information for unionricambi.it
_____
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host unionricambi.it, Searched 0 pages containing 0 results

Gathered TCP Port information for 95.110.164.90
```

Port	State
21/tcp	open
22/tcp	open

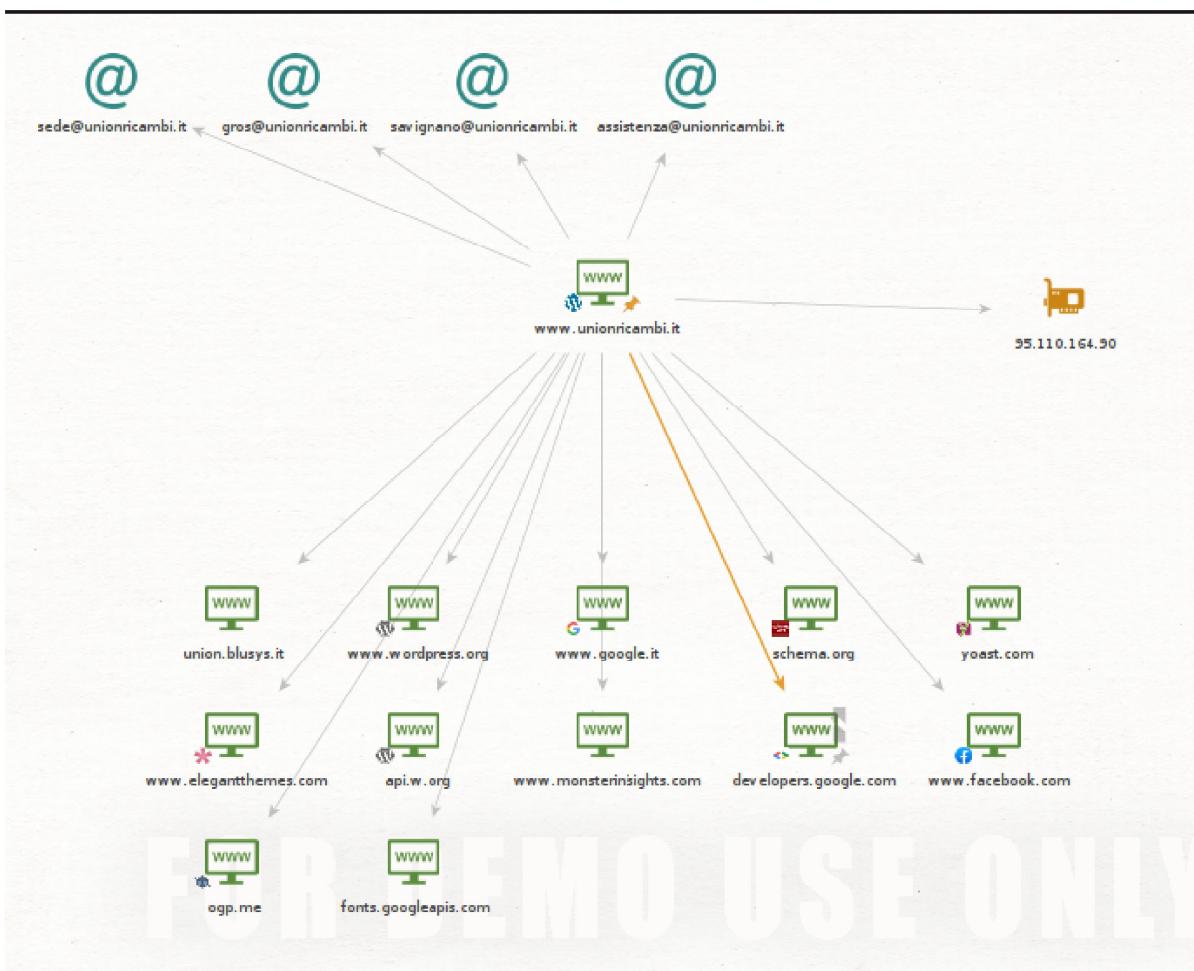
```

Port      State
21/tcp    open
22/tcp    open
53/tcp    open
80/tcp   savignano@unionricambi.it open
110/tcp   open
143/tcp   open

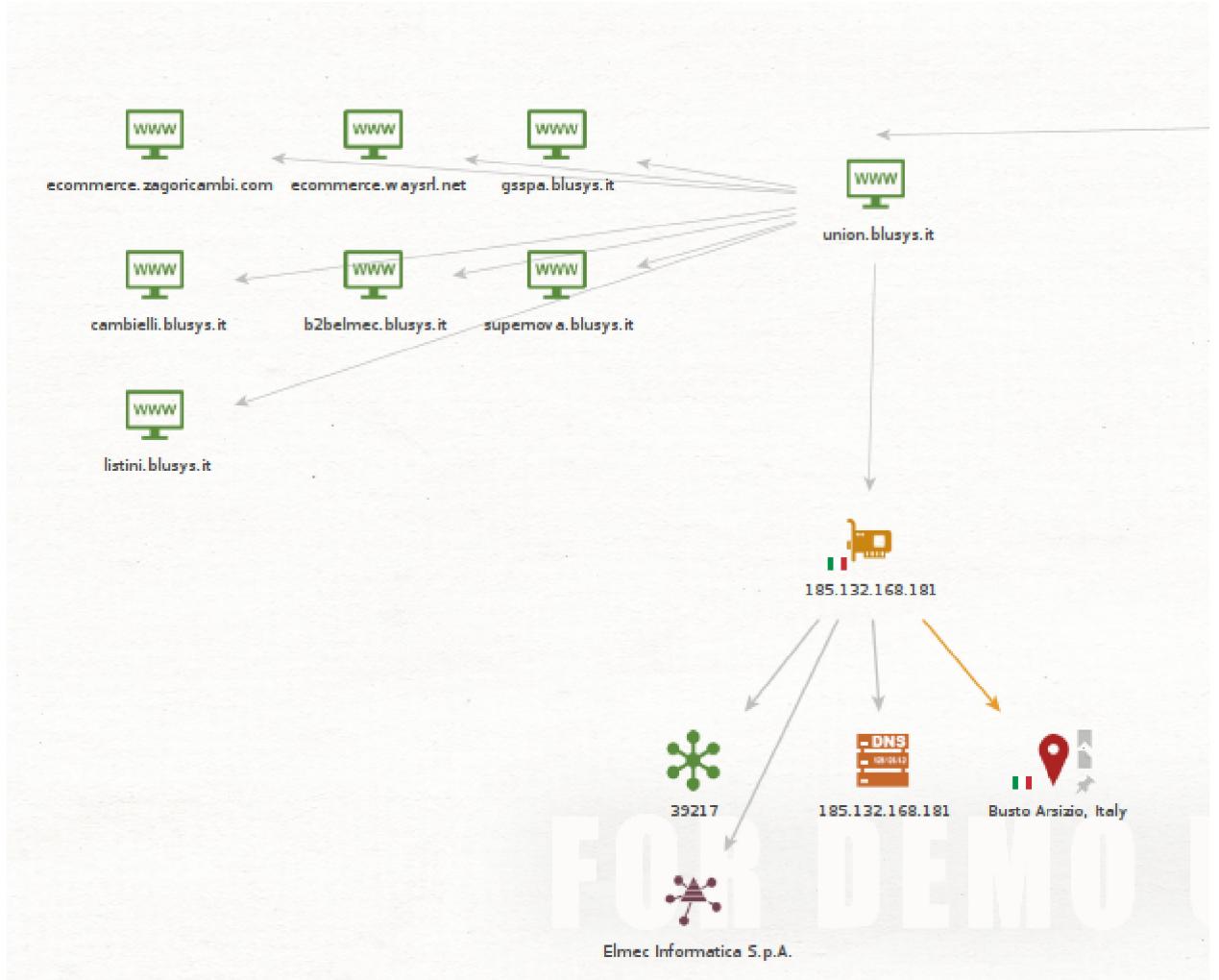
Portscan Finished: Scanned 150 ports, 0 ports were in state closed

```

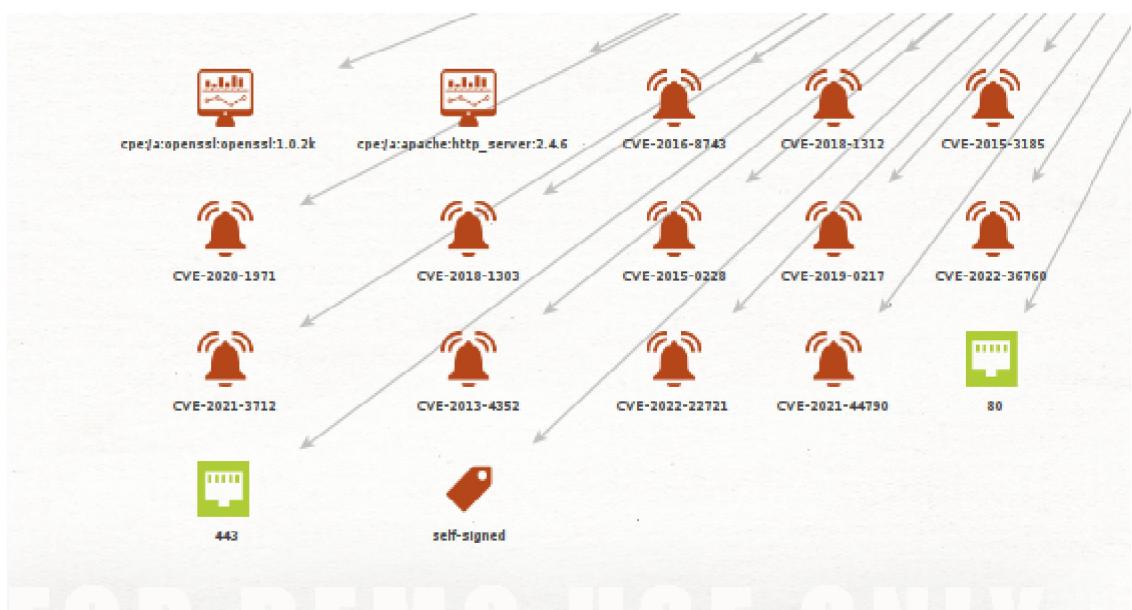
Info con Maltego



Possiamo vedere le mail collegate, un indirizzo ip e i siti collegati, dato che sappiamo che union.blusys.it è il settore e-commerce quindi cerchiamo qualche altro dato:



Analizzo le vulnerabilità sull'ip su maltego



theHarvester:

```
(alessio㉿kali)-[~]
$ theHarvester -d www.unionricambi.it -b otx
*****
* [L|_|- \^ /--|-=V\|X=|[L|-/-|-]*
* |L|- \^ /--|-=V\|X=|[L|-/-|-]*
* |L|- \^ /--|-=V\|X=|[L|-/-|-]*
* \|-|-|v|-|-|||v|\|X=|[L|-/-|-]*
* 
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
* 
*****
[*] Target: www.unionricambi.it
[*] Searching Otx.
[*] IPs found: 1
95.110.164.90
[*] No emails found.
[*] No hosts found.
```

Recon-NG

```
_____
UNIONRICAMBI.IT
_____
[*] URL: http://whois.arin.net/rest/pocs;domain=unionricambi.it
[*] No contacts found.
[recon-ng][default][whois_pocs] > options set SOURCE conad.it
SOURCE => conad.it
[recon-ng][default][whois_pocs] > run
```

```
[recon-ng][default][ghdb] > options set SOURCE unionricambi.it
SOURCE => unionricambi.it
[recon-ng][default][ghdb] > run
```

```
_____
UNIONRICAMBI.IT
_____
[recon-ng][default][ghdb] > options set SOURCE union.blusys.it
SOURCE => union.blusys.it
[recon-ng][default][ghdb] > run
```

```
_____
UNION.BLUSYS.IT
_____
[recon-ng][default][ghdb] > back
[recon-ng][default] > back
```