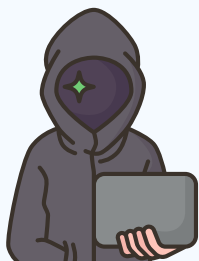


**VAN ZWAM
ARJEN**

#ByteRebels

REPORT

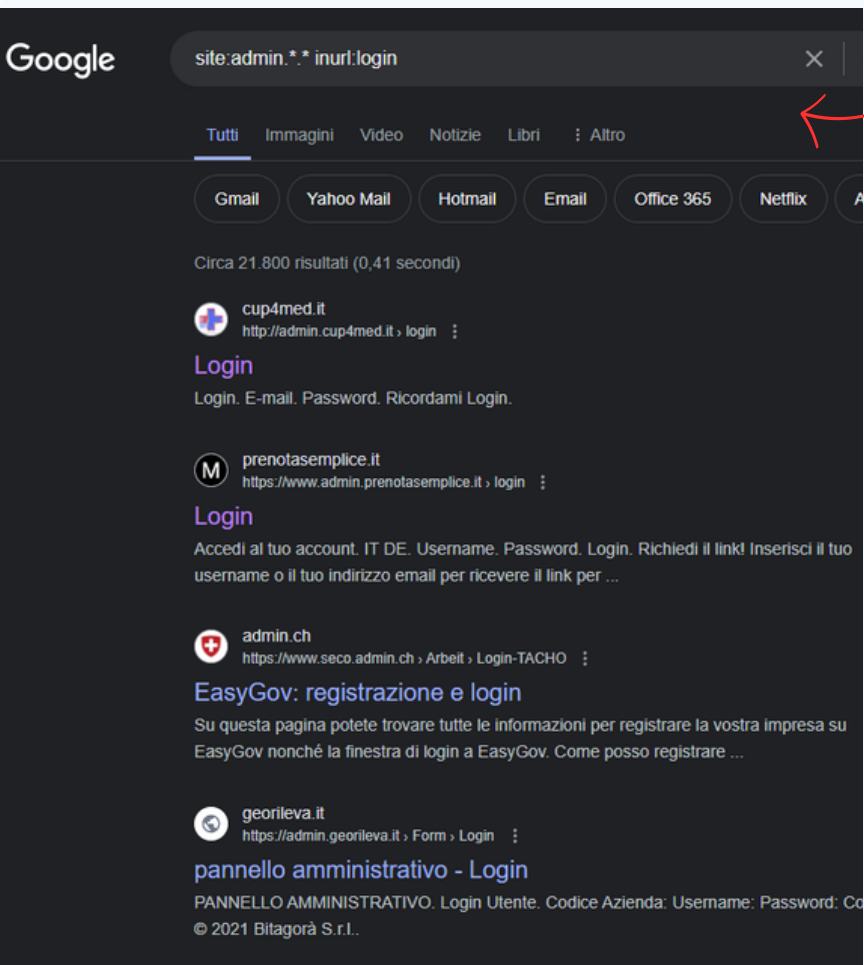
RACCOLTA INFORMAZIONI



TARGET:

PrenotaSemplice.it

SCELTA DEL TARGET

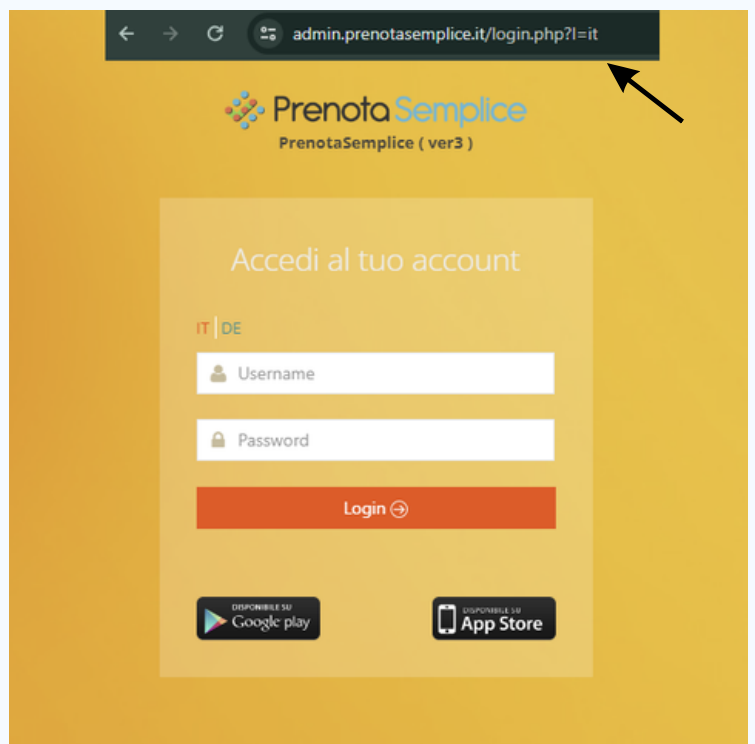


Google Dork

Tramite **Google Hacking** ho voluto scegliere un target che combaciava con un Dork recuperato dall'**Exploit Database**

Controllo del link

Il link trovato tramite il **Google Dork** ha evidenziato un form d'accesso per un pannello di controllo **admin**



PUOI AVERE ENTRAMBI, NELLA STESSA APP

proponi ai clienti i tuoi prodotti, mentre prenotano i tuoi servizi.

Con Prenota Semplice e Ordina Semplice offrirai la possibilità ai tuoi clienti di prenotare i tuoi servizi e di acquistare i tuoi prodotti con un'unica applicazione.

A chi si rivolge?

La flessibilità permette a PrenotaSemplice e OrdinaSemplice di adattarsi ad ogni tipologia di esercente. **E' l'unica App di prenotazione multisettoriale:** può essere utilizzato da **palestre, ristoranti, scuole guida, autolavaggi, centri revisione, gommisti, professionisti sanitari.**

Tutti coloro che lavorano su prenotazione e vogliono anche un sistema e-commerce potente e semplice, che aumenti le vendite in modo mirato.

INFO SUL TARGET

Il target scelto totalmente a **random** è una startup di un'applicazione iOS/Android, l'ho ispezionata con vari Tool e come prima cosa ho scoperto l'**IP** con **nslookup**

```
File Actions Edit View Help
(kali@kali)-[~]
$ nslookup
> prenotasemplice.it
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:   prenotasemplice.it
Address: 195.231.70.7
>
```

Al termine ho anche controllato **informazioni** base, come il *nome* dell'organizzazione, l'*hosting provider*, l'*indirizzo* della sede, la *data di creazione* e l'*ultimo Update* del sito in questione.

```
File Actions Edit View Help
(kali@kali)-[~]
$ whois prenotasemplice.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:      prenotasemplice.it
Status:      ok
Signed:      no
Created:     2016-09-14 09:05:05
Last Update: 2023-09-30 00:57:53
Expire Date: 2024-09-14

Registrant
Organization: itcsystem srl
Address:      via avvogadro 6
              BOLZANO
              39100
              BZ
              IT
Created:      2016-09-14 09:05:04
Last Update: 2016-09-14 09:05:04

Admin Contact
Name:         giovanni bonanno
Organization: itcsystem srl
Address:      via resia, 31, 6
              BOLZANO
              39100
              BZ
              IT
Created:      2016-09-14 09:05:04
Last Update: 2016-09-14 09:05:04

Technical Contacts
Name:         giovanni bonanno
Organization: itcsystem srl
Address:      via resia, 31, 6
              BOLZANO
              39100
              BZ
              IT
Created:      2016-09-14 09:05:04
Last Update: 2016-09-14 09:05:04

Registrar
Organization: Aruba s.p.a.
```

TECNOLOGIE WEB

Tramite la ricerca sul mitico
Shodan.io si evidenziano le
tecnologie utilizzate:

Prototype
RequireJS

PORTE

Lo **scan** delle porte aperte è già
stato effettuato, ma volendo si può
fare con lo script in python.

Le porte aperte sono:
21 - 80 - 443 - 8443

VULNERABILITA'

Tramite Shodan il sito **NON** presenta
vulnerabilità note

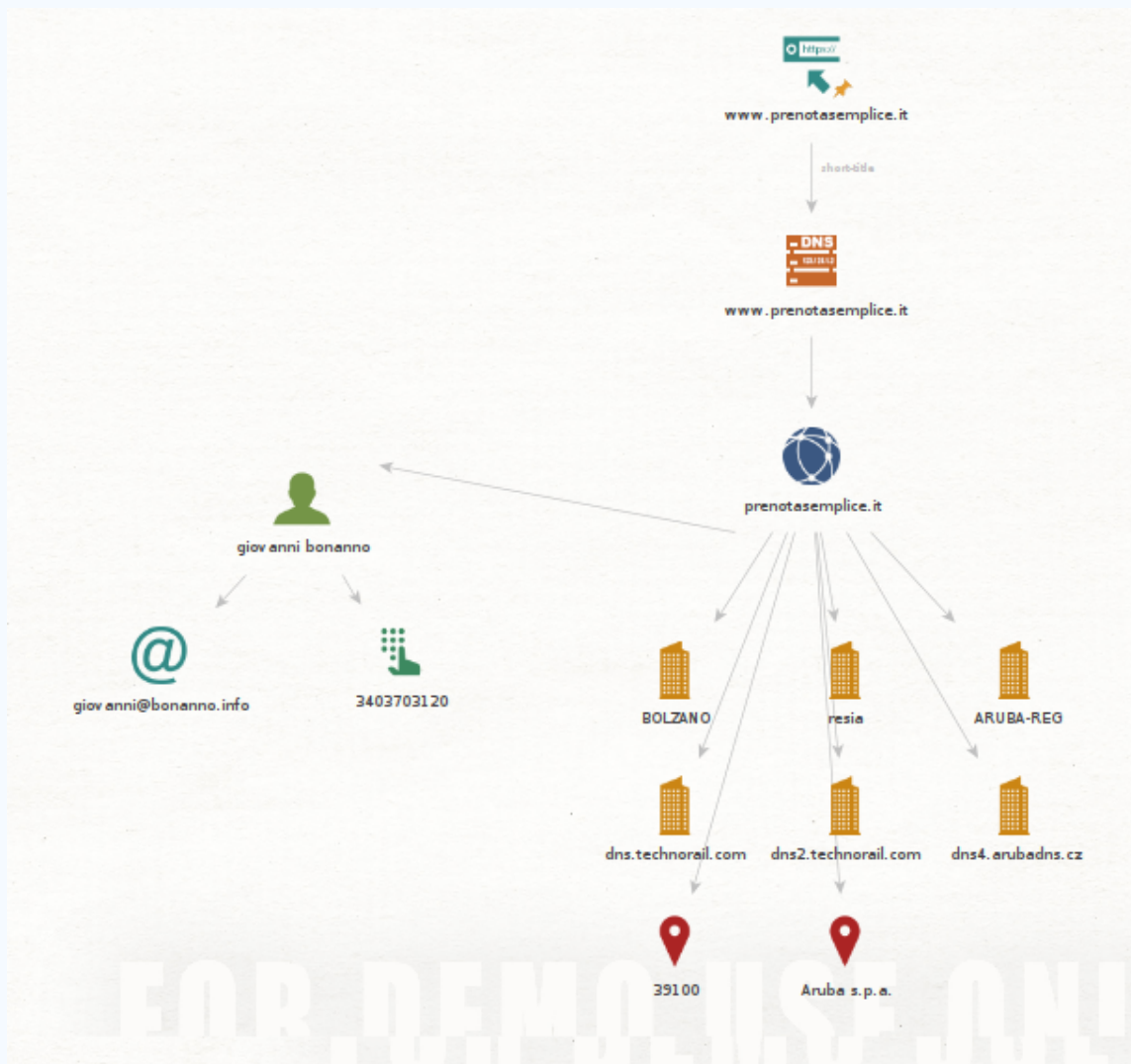
Per un lavoro più meticoloso ho
provato col mio script e ho trovato
altre porte aperte

The screenshot shows the Shodan.io host page for IP 195.231.70.7. The page is divided into several sections:

- General Information:** Hostnames (nu000187arubabiz.net), Domains (ARUBABIZ.NET), Country (Italy), City (Ponte San Pietro), Organization (Aruba S.p.A. - Cloud Services IT3), ISP (Aruba S.p.A.), and ASN (AS31034).
- Open Ports:** A list of open ports: 21, 80, 443, and 8443.
- Web Technologies:** JavaScript Frameworks (Prototype, RequireJS).
- Raw Data:** A section showing the output of a port scan, including the following commands recognized: CND, XCHD, CDP, XCP, SHNT, QUIT, PORT, PASV, EPRT, EPSV, ALLO, RUP, RINT, DELE, HOTH, RND, XHND, PND, XHND, PND, XHND, SIZE, SVST, HELP, HOOP, FEAT, OPTS, HOST, CLNT, AUTH, CCC, COM, ENCL, HCL, PSEZ, PROT, TYPE, STRU, MODE, RETR, STOR, STOU, APPR, REST, ABOR, RANG, USER, PASS, ACCT, REIN, LIST, HLST, STAT, SIZE, HLSD, HLST.

```
kali@kali: ~/Desktop
(kali@kali)~[~/Desktop]
$ python portscanner.py
Inserisci l'indirizzo IP del malcapitato da scansire: 195.231.70.7
Inserisci il port range da scansire (es: 1-189): 1-9000
Sto scannerizzando l'host zio pera sta chieto 195.231.70.7 dalla porta 1 alla porta 9000
*** Porta 21 - APERTA ZIO PERA ***
*** Porta 53 - APERTA ZIO PERA ***
*** Porta 80 - APERTA ZIO PERA ***
*** Porta 443 - APERTA ZIO PERA ***
```

MALTEGO



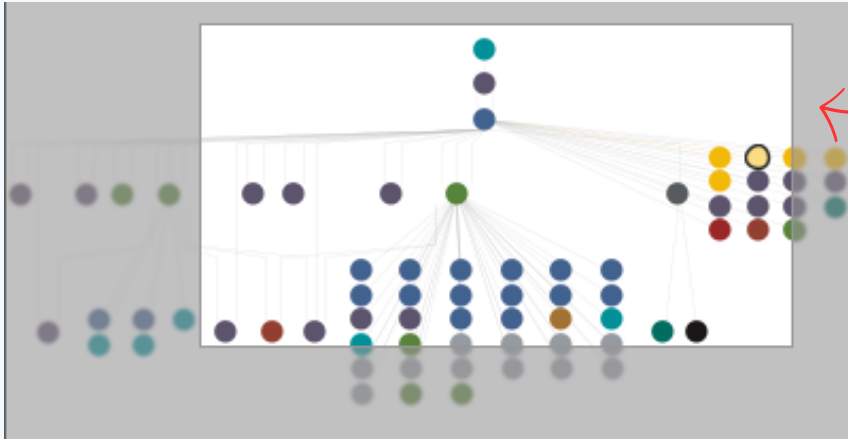
Tramite il tool **Maltego**, ho iniziato a ricostruire il sito con le informazioni inerenti ad esso estrapolando ciò che mi faceva comodo.

Ad esempio, come si vede dall'immagine, sono partito dall' **URL** (target), ho controllato il DNS con "**To DNSNames**".

A sua volta "**To Domains**", che estrae tutti i domini da un nome DNS.

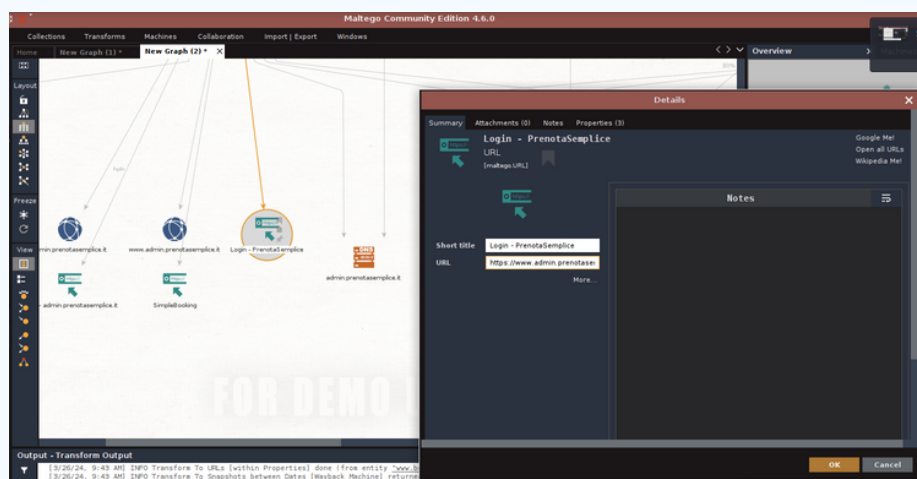
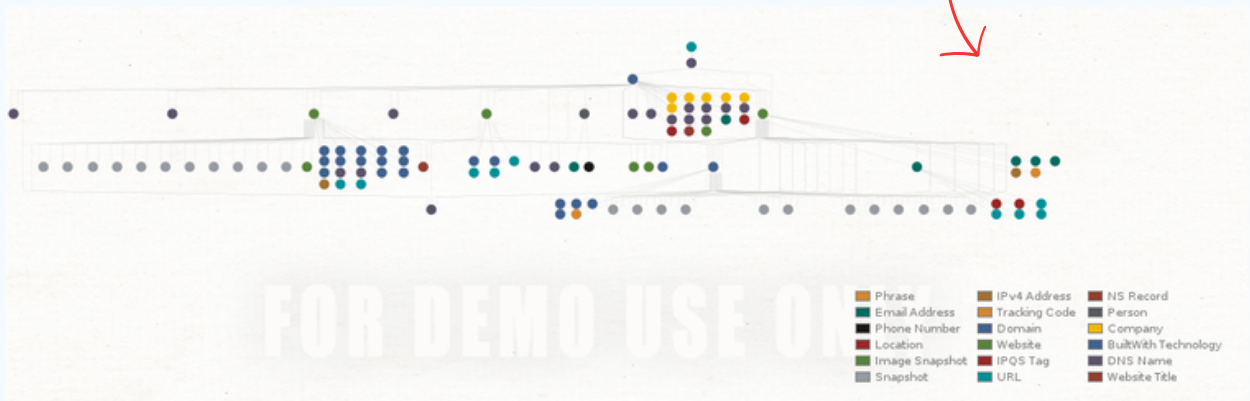
A questo punto ho utilizzato le API di IBM Watson, "**To Entities from WHOIS**" e ho trovato info utili come il proprietario del dominio, dove a sua volta ho estrapolato l'email ed il numero di cellulare con "**To email addresses**" e anche il phone number con le API's di Bing "**To phone number [BING]**"

MALTEGO



Overview

Una piccola estrapolazione grafica di ciò che sono riuscito ad ottenere con **pochi** e semplici tool



Infine ho notato che tra tutte le pagine del sito in questione appariva un altro form d'accesso **molto, molto buggato**.
Dove provando alcune credenziali l'accesso è possibile.

5.70

Webmii score

Giovanni Bonanno



Available on the App Store | Share 0

W Giovanni Bonanno (Misilmeri, 13 settembre 1913 – Viddubian, 15 giugno 1940) è stato un militare e aviatore italiano, decorato con la medaglia d'oro al valor ...

@giovannibonanno76

Via Gradenigo Sandro Bongiani Via Giovanni Linea Bus Luca Zampieri Lorenzo Paoletti Giuseppe Romeo Pietro Bruno Alessandro Grillo



Vendita Appartamento in via Giovanni Bonanno 51. Palermo. Buono ...

16 mar 2024 ... 8,5 VANI IN VIA GIOVANNI BONANNO - MQ 193 Appartamento in vendita di mq 193 in Via Giovanni Bonanno (traversa di via Libertà) piano settimo composto da ...
immobiliare.it

Cartoleria Morphese dal 1963

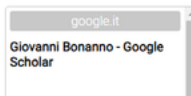
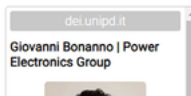
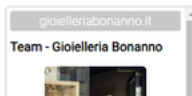
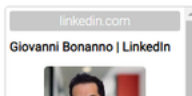
14 mar 2024 ... biglietto un'allegria contagiosa! Vieni a scoprirli: Via Giovanni Bonanno 25 - Palermo ☎ 091362306 - #CartoleriaMorphese #Cartoleria ...
facebook.com

Vendita Appartamento in via Giovanni Bonanno 67. Palermo. Buono ...

7 mar 2024 ... Questo prestigioso appartamento è ubicato al sesto piano (penultimo) dello stabile posto ad angolo fra la via Giovanni Bonanno e la via della Libertà.
immobiliare.it



powered by Google Custom Search



WEBMII

Questa volta **Webmii** non ha prodotto risultati utili anche se come score ha ottenuto **5.70**

Dovuto dal fatto che non conosco tale persona non sono riuscito a proseguire oltre.

