

TASK:

Simulazione della fase di raccolta informazioni

Per prima cosa ho scelto il target della mia ricerca: la società automobilistica MAZDAM. Ho iniziato facendo una serie di ricerche su google. La prima è stata la query DEFINE:

define:mazda

Circa 21.200.000 risultati (0,63 secondi)

Suggerimento: Cerca risultati solo in italiano. Puoi specificare la lingua di ricerca in [Preferenze](#).

<https://en.wiktionary.org> > wiki · [Traduci questa pagina](#)

Mazda - Wiktionary

Transliteration of Avestan 𐬨𐬁𐬀𐬌𐬎𐬭𐬀 (mazdā, "wisdom"). Proper nounEdit. **Mazda**. (Zoroastrianism) Ahura **Mazda**, the supreme and transcendental god ...

[English](#) · [Etymology 2](#)

<https://www.mazda.com> > behind · [Traduci questa pagina](#)

A Story Behind the Name of "Mazda" | We are Mazda

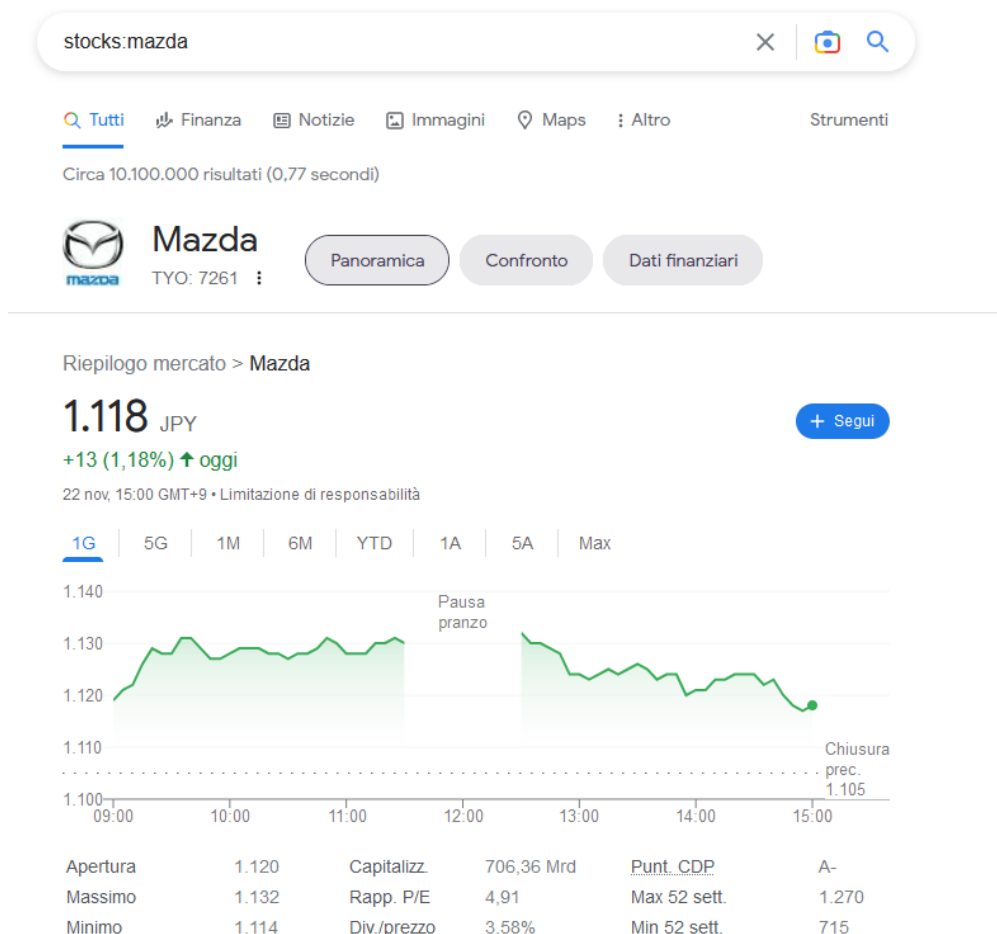
"Mazda" comes from Ahura **Mazda**, the god of harmony, intelligence and wisdom from the earliest civilization in West Asia. Key members of Toyo Kogyo interpreted ...

Mazda
Casa automobilistica

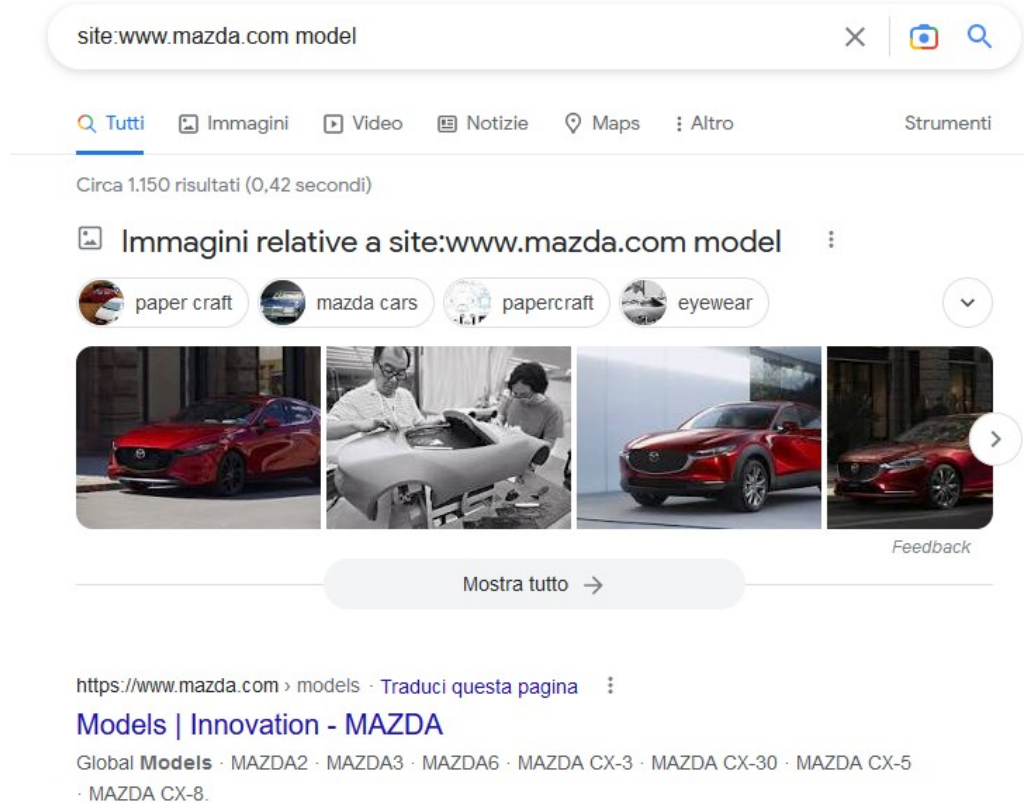
La Mazda Motor Corporation, nota semplicemente come Mazda, è una casa automobilistica giapponese con sede a Fuchū, Aki, Prefettura di Hiroshima.
[Wikipedia](#)

Fondatore: [Jujiro Matsuda](#)

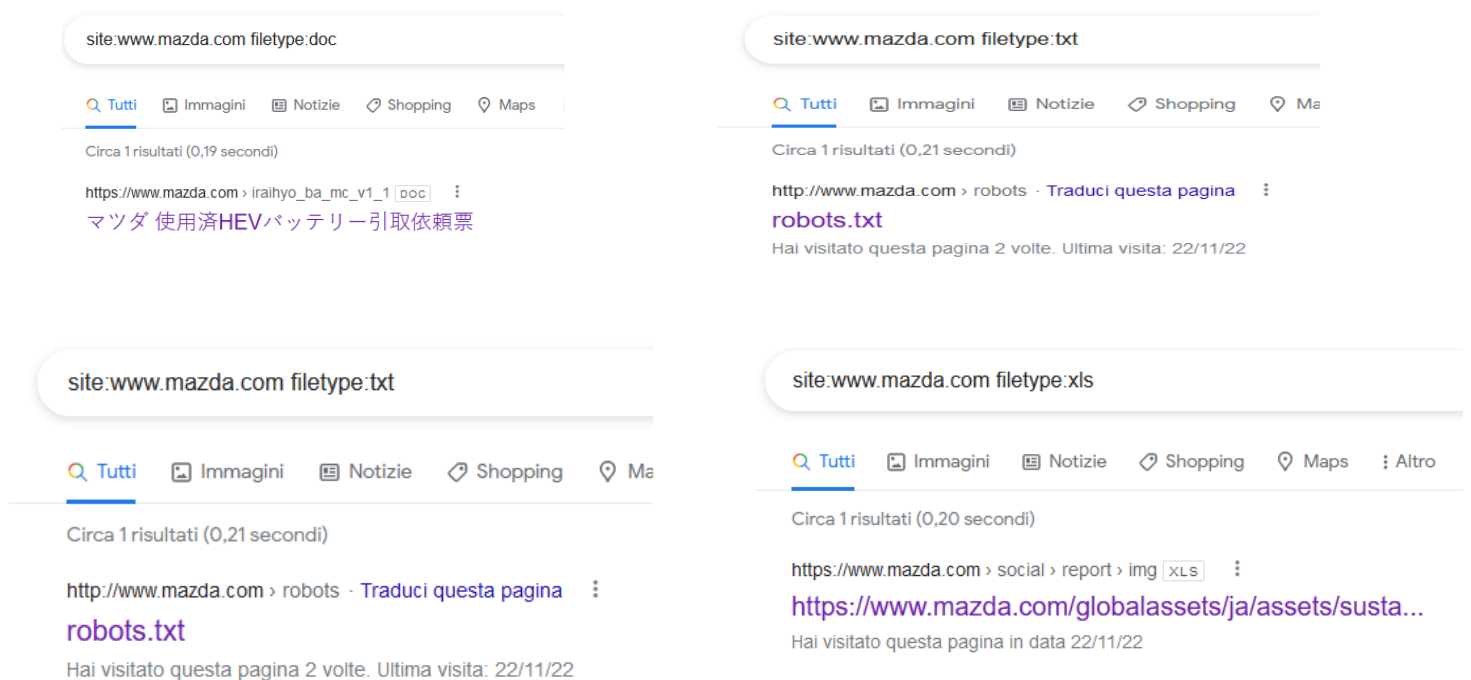
Sono andato poi a fare la query STOCKS per vedere se fosse una società quotata in borsa:



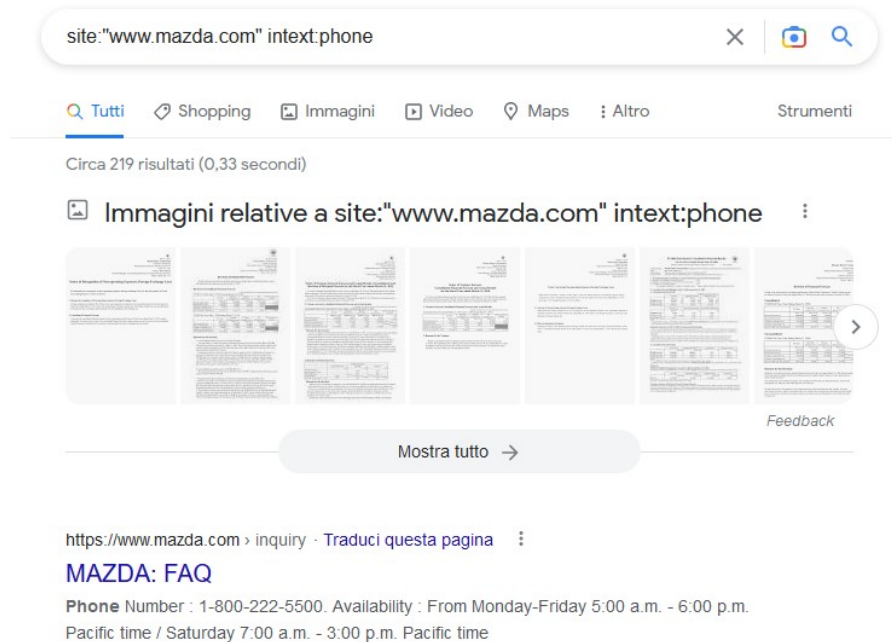
Essendo un'azienda che produce automobili sono andato a vedere se tramite query fosse possibile trovare direttamente la pagina dei modelli prodotti:



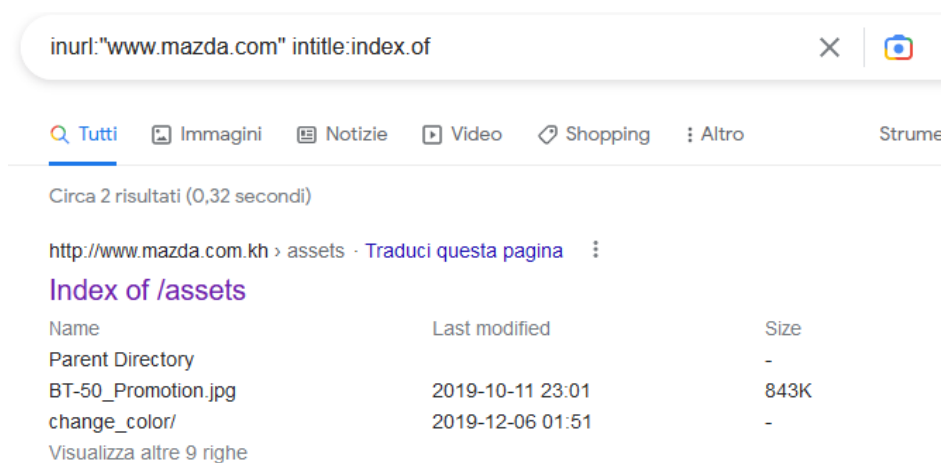
Ho poi controllato se sul loro sito principale ci fossero file scaricabili e questo è stato il risultato:



Sempre tramite query sono andato a cercare un numero di telefono che fosse contenuto nel sito web. Ho provato prima con la query phonebook:www.mazda.com ma non ho avuto risultati. Ho quindi deciso di provare con un'altra query che mi ha dato questo risultato:

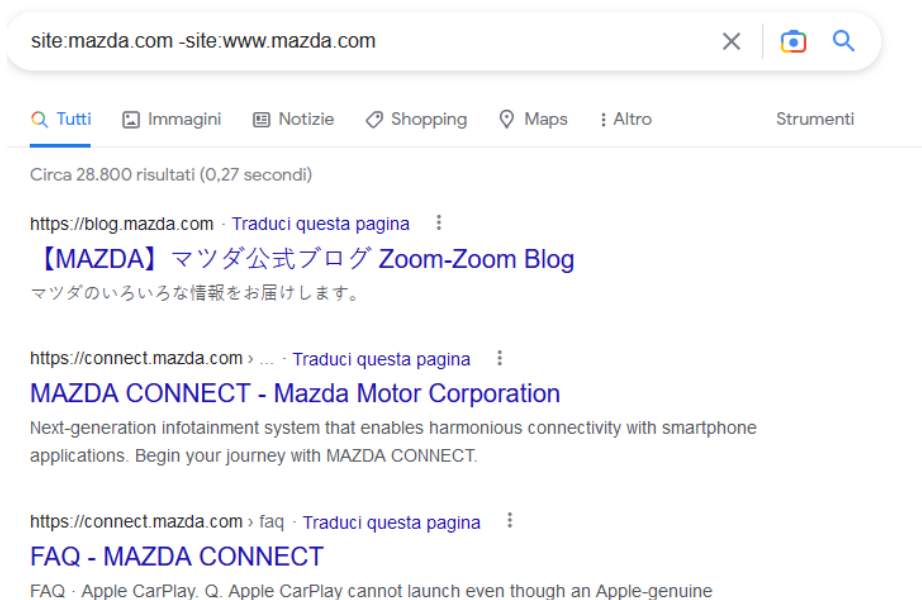


ottenendo così un numero di assistenza. Ho proseguito cercando cartelle accessibili sul server ottenendo questo risultato:



Inizialmente avevo la possibilità di accedere e girare tra le varie cartelle che non contenevano file vitali. Successivamente non mi è stato più possibile e mi ha dato errore 403.

Sono poi andato a cercare tutti i sottodomini di www.mazda.com sempre tramite query con google ottenendo questo risultato:



A questo punto ho chiuso le mie ricerche tramite l'utilizzo di google e sono passato ad usare i tool presenti su Kali. Il primo che ho utilizzato è stato theHarvester, andando a cercare il dominio mazda.com e utilizzando come fonte duckduckgo:

```
(kali㉿kali)-[~]
$ theHarvester -d mazda.com -b duckduckgo
*****
*
* theHarvester
*
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: mazda.com

[*] Searching Duckduckgo.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 5

newsroom.mazda.com:23.33.67.96
www.mazda.com:23.33.67.96
www2.mazda.com:23.33.67.96
```

Ho quindi utilizzato l'utility whois:

```
(kali@kali)-[~]
$ whois mazda.com
Domain Name: MAZDA.COM
Registry Domain ID: 1132887_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.lapi.net
Registrar URL: http://www.lapi.net
Updated Date: 2021-11-30T11:00:11Z
Creation Date: 1995-03-17T05:00:00Z
Registry Expiry Date: 2023-03-18T04:00:00Z
Registrar: IAPI GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@lapi.net
Registrar Abuse Contact Phone: +49.68949396850
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS2.MAZDA.CO.JP
Name Server: RX7.MAZDA.CO.JP
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-11-22T14:43:42Z <<<
```

Sono poi passato ad utilizzare recon-ng con il modulo “whois_poc” ma non ho trovato alcuna informazione utile:

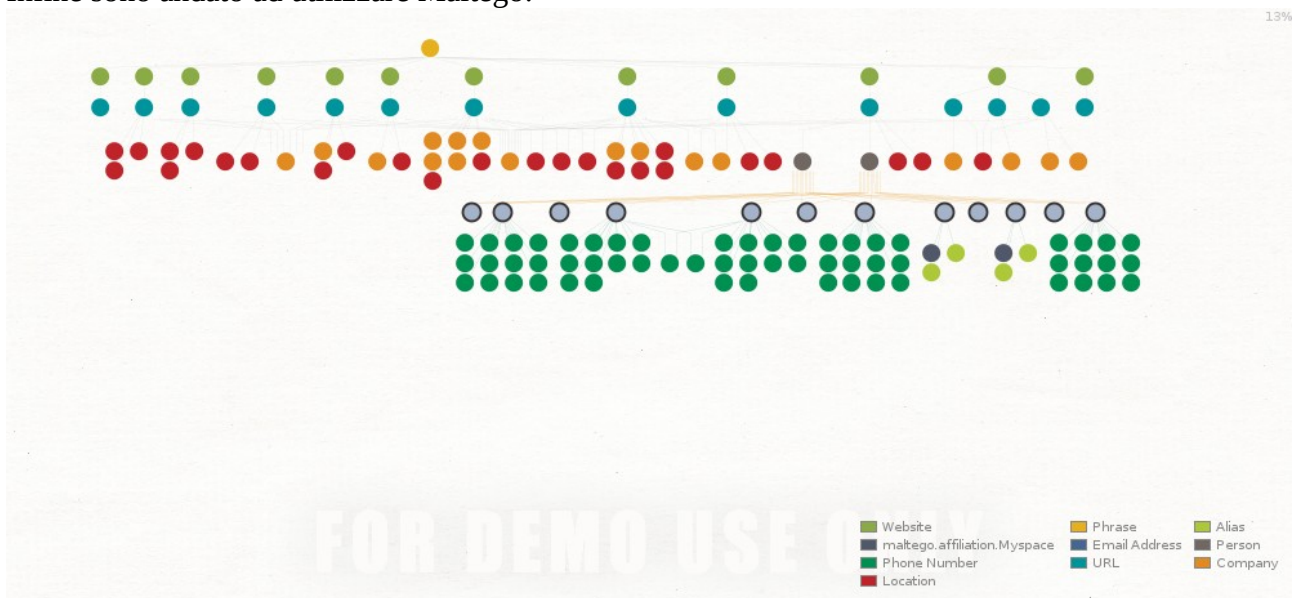
```
MAZDA.COM

[*] URL: http://whois.arin.net/rest/pocs;domain=mazda.com
[*] No contacts found.
[recon-ng][default][whois_pocs] > options set SOURCE www.mazda.com
SOURCE => www.mazda.com
[recon-ng][default][whois_pocs] > run

WWW.MAZDA.COM

[*] URL: http://whois.arin.net/rest/pocs;domain=www.mazda.com
[*] No contacts found.
```

Infine sono andato ad utilizzare Maltego:



Partendo dal cerchio giallo, che è www.mazda.com, sono passato a 12 siti web legati a lui. Da qui continuando ad aggiungere sono riuscito ad arrivare fino ad alcuni numeri di telefono ed indirizzi email di dipendenti.