

# Esercizio OSINT – Target: Avast

## *Obiettivo:*

*Simulare una fase di Information Gathering su un target reale utilizzando fonti pubbliche e strumenti OSINT per ricavare e rappresentare informazioni rilevanti.*

---

## PASSO 1 – Selezione del Target

- *Target scelto: Avast Software s.r.o.*
- *Dominio principale: [avast.com](https://www.avast.com)*
- *Settore: Cybersecurity / Antivirus*
- *Sede: Praga, Repubblica Ceca*

**Motivazione:** Avast è un'azienda globale attiva nel campo della sicurezza informatica, con infrastruttura pubblicamente visibile, numerosi contatti aziendali, un sito attivo, e presenza in vari strumenti OSINT.

# PASSO 2: Raccolta iniziale di informazioni

## QUERY SU GOOGLE:


*Ho iniziato inserendo alcune query sul motore di ricerca Google per cercare qualche documento, email e informazioni circa il CEO dell'azienda.*

**site:avast.com**

**filetype:pdf site:avast.com** → per simulare la ricerca di documenti aziendali

filetype:pdf site:avast.com


Tutti Immagini Video Video brevi Libri Web Notizie Altro



Avast  
https://files.avast.com › files › security-whitepaper PDF

Avast Passwords Security Model


Your Master Password – which only you know and which is not stored anywhere on your device or on Avast's servers – unlocks Avast Passwords on your device ...



Avast  
https://files.avast.com › files › documentation › b... PDF

avast! BackUp-Benutzerhandbuch für Windows


Kapitel 3: Verwenden des Fensters Einstellungen..... 11. Backupsätze.



Avast  
http://files.avast.com › backup\_full\_user\_guide\_nl PDF

Gebruikershandleiding voor avast! BackUp voor Windows


Hoofdstuk 3: Het venster Instellingen gebruiken..... 11. Inzicht in back-upsets.



Avast  
https://files.avast.com › files › documentation › b... PDF

avast! BackUp for Windows User Guide


Chapter 3: Using the Settings Window..... 11. Understanding Backup Sets.



Avast  
http://files.avast.com › backup\_full\_user\_guide\_es PDF

Guía del usuario de avast! BackUp para Windows


Capítulo 3: Uso de la ventana Configuración..... 11. Descripción de los conjuntos de copia de ...



Avast  
https://www.avast.com › besafeonline › stahnout PDF

kd yž n avštěvujete webo vé stránky


a ochráníte tak nejen firemní majetek, ale i sami sebe. Chraňte firmu, instituci i sebe. KD. YŽ INSTALUJETE SOFTW. ARE AAKTU.



Avast  
http://files.avast.com › backup\_full\_user\_guide\_it PDF

Guida utente avast! BackUp per Windows

Capitolo 3: Uso della finestra Impostazioni..... 11. Informazioni sui set di backup.



Avast  
http://files.avast.com › backup\_full\_user\_guide\_fr PDF

Guide d'utilisation de avast! BackUp pour Windows


Chapitre 3: Utilisation de la fenêtre Paramètres..... 11. Fonctionnement des jeux de sauvegarde.

**inurl:contact site:avast.com** → per contatti e riferimenti email

inurl:contact site:avast.com


Tutti Immagini Video Notizie Video brevi Web Libri Altro ▾

Film EDreams Wizz Air DPD Digi Disneyplus com Eyes ING

 Avast  
https://support.avast.com › contact · Traduci questa pagina ⋮

### Contact Avast Support - Avast Phone Number, and Chat ...

**Request help from Avast.** Describe your issue. Quick solutions. Contact options. Connect with us. What can we help you with? Unsubscribe.

 Avast  
https://support.avast.com › it-it › article › contact-support ⋮

### Come contattare il Supporto Avast

2 giu 2022 — Il **Supporto Avast risponde solitamente entro 2 giorni lavorativi**. I tempi di risposta possono tuttavia variare in base al carico di lavoro, alla ...


**"CEO of Avast"** → per identificare la persona chiave

"CEO of Avast" X 🔊 📷 🔍

Tutti Immagini Notizie Video Video brevi Web Libri Altro ▾ Strumenti ▾


🌟 AI Overview

The current CEO of Avast is **Ondřej Vlček**. He assumed the role in 2019, succeeding Vince Steckler. Prior to becoming CEO, Vlček held positions as Executive Vice-President & General Manager, Consumer, and Chief Technology Officer. ⓘ



New Avast CEO Ondrej Vlcek Looks Ahead | Avast  
1 lug 2019  
Avast Blog ⋮

**intext:"@avast.com"** → per estrarre indirizzi email pubblici

 Avast  
https://www.avast.com › it-it › privacy-policy ⋮

### Informativa sulla privacy generale

L'utente potrà sempre contattarci tramite e-mail all'indirizzo **dpo@avast.com**. Si prega di indicare "RICHIESTA RELATIVA ALLA PRIVACY" nella riga dell'oggetto ...

# WHOIS

Ho poi continuato eseguendo il comando whois [avast.com](https://avast.com) per estrarre informazioni di registrazione dominio.

Le informazioni ricavate sono le seguenti:

*Registrar: MarkMonitor Inc.*

*Data creazione dominio: 06/10/1997*

*Data scadenza: 20/09/2030*

*Name servers (Akamai): A1-182.AKAM.NET, ecc.*

*Protezioni attive: Transfer/Delete/Update Prohibited*

```
(kali@kali)-[~] sshark - base64_ca...
$ whois avast.com
Domain Name: AVAST.COM
Registry Domain ID: 528943_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-12-09T19:05:21Z
Creation Date: 1997-10-06T04:00:00Z
Registry Expiry Date: 2030-09-20T22:05:36Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: A1-182.AKAM.NET
Name Server: A11-66.AKAM.NET
Name Server: A13-65.AKAM.NET
Name Server: A20-66.AKAM.NET
Name Server: A26-67.AKAM.NET
Name Server: A6-67.AKAM.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-28T12:32:59Z <<<
```

# SHODAN

Ho proseguito poi eseguendo una ricerca su Shodan utilizzando la seguente query:

*org:"Avast Software s.r.o."*

*Totale host rilevati: 1.211.574*

*Paesi principali:*

*Repubblica Ceca: 421.625*

*USA: 393.229*

*UK: 377.729*

*Porte più comuni:*

*4040, 8575, 1311, 1024, 8200*

*Tecnologie rilevate:*

*nginx*

*CiscoSystems*

*Check Point Firewall*

**Host associati ad Avast trovati:**

IP Address	Località	Note
5.62.66.108	San Jose, USA	consumer-pool.pcrdn.net
5.62.42.224	Londra, UK	vpn-vityru-prod.avast.com
5.62.66.144	San Jose, USA	consumer-pool.pcrdn.net
5.62.66.76	San Jose, USA	consumer-pool.pcrdn.net

Nota: gli host sono registrati su reti di tipo consumer (probabilmente per VPN, endpoint o raccolta dati) e indicano distribuzione geografica dei servizi Avast.

Questo mi ha restituito oltre **1.200.000 risultati**, con host distribuiti principalmente in **Repubblica Ceca, Stati Uniti e Regno Unito**.

Tra le informazioni utili raccolte:

- Host attivi con IP appartenenti ad Avast, come 5.62.66.108, 5.62.42.224 e altri

- Alcuni IP appartenevano a pool di rete consumer, probabilmente associati a servizi VPN o raccolta dati
- Sono emerse porte aperte comuni (es. 4040, 8575) e tecnologie utilizzate come nginx e Cisco Systems

Questo tipo di informazione è particolarmente rilevante per analisi sulla superficie esposta e per la ricostruzione di eventuali infrastrutture tecniche.

[SHODAN](#)
[Explore](#)
[Downloads](#)
[Pricing](#)

org:"Avast Software s.r.o."

TOTAL RESULTS

1,211,574

TOP COUNTRIES

Czechia	421,625
United States	393,229
United Kingdom	377,729
Singapore	17,812
Israel	1,160
<a href="#">More...</a>	

TOP PORTS

4040	275
8575	195
1311	190
1024	189
8200	188
<a href="#">More...</a>	

TOP PRODUCTS

nginx	455
ciscoSystems	60
Check Point Firewall	24
Check Point SVN foundation httpd	11
Zscaler Cloud Services	11
<a href="#">More...</a>	

[View Report](#)
[View c](#)

Access Granted: Want to get more out of your exist

5.62.56.108

r-108-56-62-5.consumer-pool.prcdn.net  
AVAST Software s.r.o.  
United States, San Jose

No data returned

5.62.42.224

vpn-virgww-prod-095.lon1.ff.avast.com  
AVAST Software s.r.o.  
United Kingdom, London

No data returned

5.62.62.240

r-240-62-62-5.consumer-pool.prcdn.net  
AVAST Software s.r.o.  
United Kingdom, London

No data returned

5.62.56.144

r-144-56-62-5.consumer-pool.prcdn.net  
AVAST Software s.r.o.  
United States, San Jose

No data returned

5.62.42.221

vpn-virgww-prod-092.lon1.ff.avast.com  
AVAST Software s.r.o.  
United Kingdom, London

No data returned

5.62.56.120

r-120-56-62-5.consumer-pool.prcdn.net  
AVAST Software s.r.o.  
United States, San Jose

No data returned

5.62.56.76

r-76-56-62-5.consumer-pool.prcdn.net  
AVAST Software s.r.o.  
United States, San Jose

No data returned

## PASSO 3: ANALISI MALTEGO

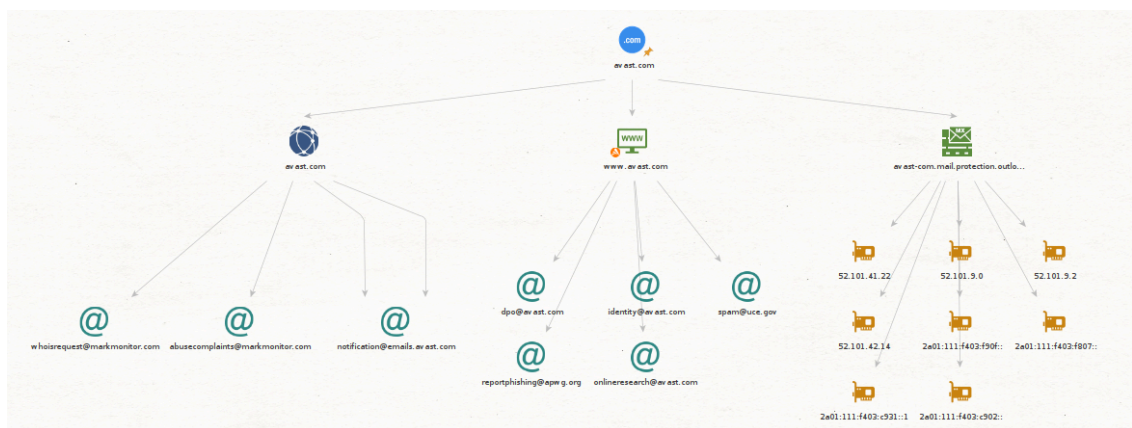
Con i dati raccolti, sono passato all'analisi e mappatura visuale utilizzando **Maltego CE** su Kali Linux. Dopo aver risolto un problema iniziale con l'interfaccia (Entity Palette vuota), ho aggiornato i Transform Pack dal Transform Hub e ho creato un nuovo grafo.

Nel grafo ho inserito:

- L'entità Company per **Avast Software s.r.o.**
- Il Domain **avast.com**
- Le Email Address trovate su Google
- La Person associata al CEO **Ondřej Vlček**

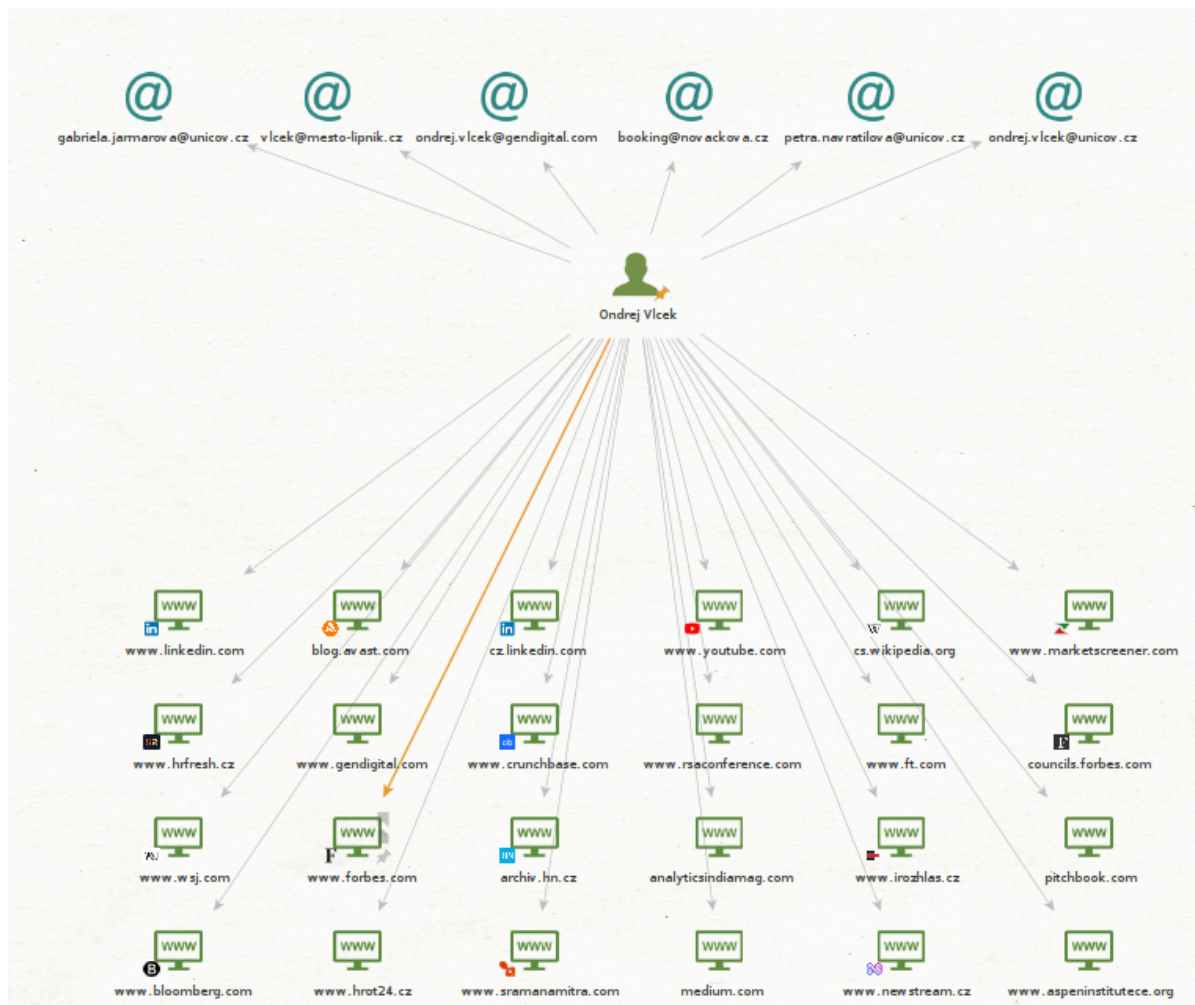
Ho applicato varie trasformazioni alle entità:

- Sul dominio **avast.com**, la trasformazione To DNS Name ha restituito sottodomini utili come **support.avast.com**, **vpn.avast.com** e **www.avast.com**
- Su questi DNS ho applicato altre trasformazioni per cercare IP e ulteriori domini, ma non sono emersi indirizzi IP specifici a causa della protezione fornita da Akamai
- Il record **avast-com.mail.protection.outlook.com** ha confermato che Avast utilizza **Microsoft 365** per la posta elettronica



Infine, ho aggiunto l'ex CEO **Ondřej Vlček** al grafo come persona. Anche se le trasformazioni verso social network o email personali non hanno restituito risultati, l'aggiunta è stata utile per stabilire il legame tra la leadership aziendale e il dominio.





## Considerazioni finali

L'intero processo di raccolta dati e analisi ha permesso di ottenere un quadro dettagliato di Avast dal punto di vista OSINT. Nonostante l'uso di protezioni avanzate (CDN, offuscamento IP), è stato possibile:

- Identificare sottodomini attivi
- Trovare indirizzi email pubblici
- Visualizzare le connessioni tra dominio, servizi e personale
- Rilevare parte dell'infrastruttura tecnica esposta su Shodan

Il grafo finale di Maltego evidenzia chiaramente i nodi centrali e le loro relazioni, ed è sempre pronto per essere ampliato in futuro con ulteriori fonti.