

# Fase di raccolta informazioni

Traccia: Nell'esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta.

Lo scopo di questo esercizio è più che altro familiarizzare con i tool principali della fase di information gathering, quali:

Google, per la raccolta passiva delle info

Maltego

Lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato: il target, le query utilizzate (dove applicabile) e i risultati ottenuti

**Target:** beretta.com

"La fabbrica d'armi Pietro Beretta, nata nel 1526, produce pistole, fucili, carabine e accessori pensati per chi pratica caccia e tiro a volo."

**Tools utilizzati:**

Google

Shodan

Whois

Recon-ng

Maltego

**Google:**

Controllo di Sottodomini Potenzialmente Vulnerabili

site:\*.beretta.com

Cerca tutti i sottodomini di beretta.com per identificare le aree meno sicure.

La ricerca restituisce una varietà di risultati dal sito web di Beretta. Tra i risultati trovati, ci sono diverse categorie di prodotti e informazioni:

- **Prodotti:** La ricerca mostra una vasta gamma di prodotti offerti da Beretta, come pistole, fucili, carabine e accessori correlati. Questi includono sia armi per scopi sportivi che per la difesa personale.
- **Informazioni sull'Azienda:** Sono presenti anche pagine che descrivono la storia e il background dell'azienda Beretta, una delle più antiche fabbriche di armi da fuoco al mondo.
- **Supporto e Servizi:** Alcuni link portano a sezioni del sito dedicate al supporto clienti, manuali di prodotto, informazioni sulla manutenzione delle armi e opzioni di assistenza.

- **Novità e Eventi:** Ci sono anche aggiornamenti sugli ultimi prodotti, innovazioni tecnologiche, eventi sponsorizzati da Beretta e notizie relative all'industria delle armi da fuoco.
- **Negozio Online:** Viene fornito l'accesso al negozio online di Beretta, dove è possibile acquistare prodotti direttamente dal sito.
- **Informazioni Legali e di Sicurezza:** Sono disponibili anche informazioni legali riguardanti l'acquisto e l'uso responsabile delle armi da fuoco, oltre a consigli sulla sicurezza.

Google search results for "site:beretta.com":

- Beretta - Firearms, Guns, Pistols, Rifles, Clothing, Accessories ...**  
beretta.com  
https://www.beretta.com · Traduci questa pagina
- Safety Rules and Recommendations**  
Keep Your Finger Off The Trigger Until Ready To Shoot; Never Point A Gun At Anything You Do Not Want To Shoot; Be Sure Of The Target And ...  
beretta.com  
https://eu.beretta.com › gunsafet... · Traduci questa pagina
- Il progetto Cromozero – Beretta rivoluziona la fabbricazione ...**  
Il progetto Cromozero. Beretta è pronta a rivoluzionare il mondo della fabbricazione delle armi, sostituendo la cromatura con un processo completamente green.  
beretta.com  
https://life.beretta.com › progetto

Combinazione site:beretta.com inurl:login cerca pagine di accesso che potrebbero essere vulnerabili ad attacchi.

Google search results for "site:beretta.com inurl:login":

- Login**  
beretta.com  
https://my.beretta.com › ciam › login › ciam
- Affiliate Login**  
User Name Password Remember Me? Forgot Password? Not a publisher?  
beretta.com  
https://affiliates.beretta.com › ... · Traduci questa pagina
- Forgot Password**  
Loading. ×Sorry to interrupt. CSS Error. Refresh. CIAM. email. Reset password. Login. Italian. Caricamento.  
beretta.com  
https://my.beretta.com › ciam › login › ForgotPassword

Combinazione site:beretta.com filetype:txt cerca fogli di testo che potrebbero contenere informazioni sensibili.

Google search results for "site:beretta.com filetype:txt":

- robots.txt**  
beretta.com  
https://www.beretta.com › robots · Traduci questa pagina

```
Sitemap: https://www.beretta.com/de-at/sitemap.xml
Sitemap: https://www.beretta.com/en-be/sitemap.xml
Sitemap: https://www.beretta.com/en-bg/sitemap.xml
Sitemap: https://www.beretta.com/en-cy/sitemap.xml
Sitemap: https://www.beretta.com/en-cz/sitemap.xml
Sitemap: https://www.beretta.com/de-de/sitemap.xml
Sitemap: https://www.beretta.com/en-dk/sitemap.xml
Sitemap: https://www.beretta.com/en-ee/sitemap.xml
Sitemap: https://www.beretta.com/es-es/sitemap.xml
Sitemap: https://www.beretta.com/en-fi/sitemap.xml
Sitemap: https://www.beretta.com/fr-fr/sitemap.xml
Sitemap: https://www.beretta.com/en-gb/sitemap.xml
Sitemap: https://www.beretta.com/en-gr/sitemap.xml
Sitemap: https://www.beretta.com/en-hr/sitemap.xml
Sitemap: https://www.beretta.com/en-hu/sitemap.xml
Sitemap: https://www.beretta.com/en-ie/sitemap.xml
Sitemap: https://www.beretta.com/it-it/sitemap.xml
Sitemap: https://www.beretta.com/en-lt/sitemap.xml
Sitemap: https://www.beretta.com/en-lu/sitemap.xml
Sitemap: https://www.beretta.com/en-lv/sitemap.xml
Sitemap: https://www.beretta.com/en-mt/sitemap.xml
Sitemap: https://www.beretta.com/en-nl/sitemap.xml
Sitemap: https://www.beretta.com/en-pl/sitemap.xml
Sitemap: https://www.beretta.com/en-pt/sitemap.xml
Sitemap: https://www.beretta.com/en-ro/sitemap.xml
Sitemap: https://www.beretta.com/en/sitemap.xml
Sitemap: https://www.beretta.com/en-se/sitemap.xml
Sitemap: https://www.beretta.com/en-si/sitemap.xml
Sitemap: https://www.beretta.com/en-sk/sitemap.xml
```

Questo file viene utilizzato dai siti web per comunicare con i web crawler e i bots dei motori di ricerca. Questo file fornisce istruzioni su quali parti del sito possono essere indicizzate e quali parti dovrebbero essere ignorate.

Il contenuto specifico mostra:

- User-agent: \*: Indica che le regole seguenti si applicano a tutti i web crawler.
- Allow: /: Permette ai crawler di accedere e indicizzare tutto il contenuto del sito.
- Sitemap: Elenca le diverse sitemap in formato XML per varie lingue o località. Le sitemap sono utilizzate dai crawler per trovare più facilmente i contenuti del sito. Ogni URL specificato è un link diretto alla sitemap corrispondente, che contiene un elenco strutturato delle pagine disponibili per l'indicizzazione.

Cercando la sitemap per il sito italiano vedo:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<sitemapindex xmlns:xhtml="http://www.w3.org/1999/xhtml" xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
  <sitemap>
    <loc>https://www.beretta.com/it-it/products.xml</loc>
  </sitemap>
  <sitemap>
    <loc>https://www.beretta.com/it-it/categories.xml</loc>
  </sitemap>
  <sitemap>
    <loc>https://www.beretta.com/it-it/news.xml</loc>
  </sitemap>
</sitemapindex>
```

"This XML file does not appear to have any style information associated with it.": è normale dato che viene visualizzata senza alcun foglio di stile.

Analizzando ciascun elemento:

- **<sitemapindex>**: Questo è l'elemento radice che definisce che il documento è un indice sitemap, una raccolta di sitemaps separate.
- **xmlns:xhtml="http://www.w3.org/1999/xhtml"** e **xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"**: Questi sono gli spazi dei nomi XML che definiscono lo standard che il documento segue. In questo caso, segue lo standard sitemap 0.9 come definito da sitemaps.org.

All'interno del <sitemapindex>, ci sono vari <sitemap> elementi, ciascuno con un <loc> (location) elemento:

- <loc>[</loc>](https://www.beretta.com/it-it/products.xml): Questo è un URL che punta alla sitemap per i prodotti del sito italiano di Beretta.
- <loc>[</loc>](https://www.beretta.com/it-it/categories.xml): Questo è un URL che punta alla sitemap per le categorie di prodotti sul sito italiano.
- <loc>[</loc>](https://www.beretta.com/it-it/news.xml): Questo è un URL che punta alla sitemap per le sezioni di notizie del sito italiano.

Con la combinazione site:beretta.com filetype:pdf intext:"confidential" volevo cercare documenti PDF con contenuti etichettati come confidenziali. Tuttavia come per gli altri file pdf trovati mi sono imbattuta in file cancellati dal sito, consultabili andando a cercare una copia cache:

Questa è la versione html del file <https://www.beretta.com/en-us/assets/39/7/Retailer-Agreement.pdf>. Google genera automaticamente le versioni html dei documenti mentre viene eseguita la scansione del Web.

Suggerimento: Per trovare rapidamente il termine di ricerca su questa pagina, digita Ctr+F o ⌘-F (Mac) e utilizza la barra di ricerca.

#### RETAILER AGREEMENT

This Agreement (hereinafter referred to as "Agreement") is made and entered into by and between Beretta USA Corp. ("Beretta"), a Maryland corporation with offices located at 17601 Beretta Drive, Accokeek, MD 20607 (hereinafter referred to as "Manufacturer") and company with its principal place of business located at \_\_\_\_\_, (hereinafter referred to as "Retailer"). The date of this Agreement is 01/06/2020 (the "Effective Date").

WHEREAS, the Manufacturer has for many years, and is presently, engaged in the development and sale of Products throughout the world, including, but not limited to, the following: Beretta, Tikka and Sako branded non-firearms (the "Products");

products, and for other good and valid business reasons, it is the policy of Manufacturer that:

- (1) Retailer may not sell Manufacturer's products to any other retailer, re-seller, distributor, redistributor or wholesaler;
- (2) Retailer may not knowingly sell Manufacturer's products to any party intending to resell Manufacturer's products;
- (3) Retailer is authorized only to sell Manufacturer's products directly to end-user consumers; and
- (4) Retailer may not sell Manufacturer's products in bulk.

Approfondendo su ufficiocamerale.it ottengo il nome completo della ragione sociale ed altre informazioni come ad esempio il fatturato.

[ufficiocamerale.it/8268/fabbrica-darmi-pietro-beretta-spa](https://www.ufficiocamerale.it/8268/fabbrica-darmi-pietro-beretta-spa)

#### DATI DELLA SOCIETÀ - FABBRICA D'ARMI PIETRO BERETTA - S.P.A.

Partita IVA: 01541040174 - Codice Fiscale: 01541040174

Rag. Sociale: FABBRICA D'ARMI PIETRO BERETTA - S.P.A.

Indirizzo: VIA P. BERETTA 18 - 25063 - GARDONE VAL TROMPIA (BS)

Rea: 243926

PEC: f.armi.beretta@legalmail.it

Fatturato: € 317.432.096,00 (2022)

[ACQUISTA BILANCIO](#)

Dipendenti: 847 (2023)

Forma giuridica: SOCIETA' PER AZIONI CON SOCIO UNICO

Data Iscrizione: 01/08/1982

Ateco: FABBRICAZIONE DI ARMI E MUNIZIONI

Cod. Ateco: 254

Utile: € 24.348.224,00 (2022)

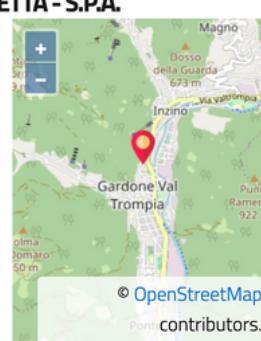
Capitale sociale: € 5.200.000,00 (2023)

Procedure e Pregiudizievoli

[ACQUISTA VISURA](#)

Camera di commercio: BS

Codice destinatario: RT4853B



Della Fabbrica d'Armi Pietro Beretta S.p.A. è possibile visualizzare gratuitamente:

- **Partita IVA e Codice Fiscale:** Numeri identificativi fiscali dell'azienda in Italia.
- **Ragione Sociale:** Il nome ufficiale dell'azienda.
- **Indirizzo:** La sede legale dell'azienda.
- **REA:** Numero di Repertorio Economico Amministrativo, un identificativo unico per ogni impresa registrata presso la Camera di Commercio.
- **PEC:** Posta Elettronica Certificata, un sistema di email legalmente riconosciuto in Italia per la corrispondenza ufficiale.
- **Fatturato:** Il ricavo totale dell'azienda per l'anno indicato.
- **Dipendenti:** Il numero di dipendenti dell'azienda nell'anno indicato.
- **Forma giuridica:** La forma legale dell'azienda, in questo caso una società per azioni con socio unico.
- **Data Iscrizione:** La data di registrazione dell'azienda presso la Camera di Commercio.
- **Ateco:** Il codice Ateco è un sistema di classificazione delle attività economiche in Italia.
- **Cod. Ateco:** Il codice specifico che identifica l'attività principale dell'azienda, in questo caso la "Fabbricazione di armi e munizioni".
- **Utile:** L'utile netto dell'azienda per l'anno indicato.
- **Capitale sociale:** Il capitale sociale dell'azienda registrato per l'anno indicato.
- **Procedure e Prejudizievoli:** Una sezione che potrebbe elencare eventuali procedure legali o problemi finanziari noti che coinvolgono l'azienda.
- **Camera di commercio:** L'abbreviazione "BS" indica la Camera di Commercio di Brescia.
- **Codice destinatario:** Un codice utilizzato per la fatturazione elettronica in Italia.

Cercando informazioni su Linkedin è possibile trovare la pagina ufficiale di Beretta con informazioni statistiche riguardanti i suoi dipendenti, nonché i collegamenti diretti ai dipendenti stessi e la sede principale della fabbrica.

The screenshot shows the LinkedIn profile of Beretta. At the top, there's a banner with a logo and a photo of people working. Below it, the company name 'BERETTA' is displayed with a small bio: 'Benvenuti nel profilo LinkedIn della più antica fabbrica d'armi esistente al mondo, basata a Gardone Valtrompia dal 1526'. It also mentions they manufacture sports articles and have 76K followers. There are buttons for '+ Segui' (Follow) and 'Invia messaggio' (Send message). The main navigation bar includes 'Home', 'Chi siamo', 'Post', 'Lavoro', and 'Persone' (which is underlined).

Key statistics are highlighted below the navigation:

- 482 utenti associati** (Associated users)
- Dove vivono**: 380 | Italy, 312 | Lombardy, Italy, 253 | Greater Brescia Metropolitan Area.
- Dove hanno studiato**: 52 | Università degli Studi di Brescia, 14 | Politecnico di Milano, 10 | Università Cattolica del Sacro Cuore.
- Cosa fanno**: 111 | Operazioni, 65 | Vendite, 44 | Amministrativo.
- Quali sono le loro competenze**: 106 | Microsoft Office, 95 | Management, 77 | Project Management.
- Cosa hanno studiato**: 32 | Economics, 22 | Business Administration and Manageme..., 17 | Marketing, 11 | Business/Commerce, General.

At the bottom, there's a search bar for 'Cerca dipendenti per qualifica, parola chiave o scuola'.

## Persone che potresti conoscere

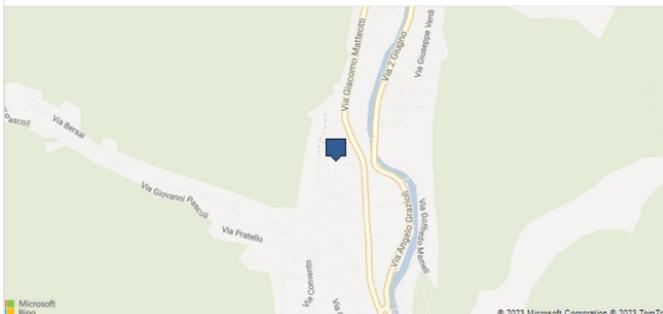
<b>Manolo Fioravanti</b> · 2° E-Commerce Specialist presso BERETTA	<b>Dario Arici</b> · 3° JDE application developer	<b>Andrea Tonola</b> · 3° Virtual prototyping engineer presso BERETTA
Andrea Cav. Pietrarota e PALOMA GOMES sono collegamenti in comune		
<a href="#">Collegati</a>	<a href="#">Collegati</a>	<a href="#">Messaggio</a>
<b>Carlo Poli</b> · 2° Process Engineer presso Fabbrica d'Armi Pietro Beretta	<b>Beatrice Lambri</b> · 3° Fashion designer	<b>Simone Leonzi</b> · 3° Magistrale in Ingegneria Meccanica, Progettazione...

## Località (1)

## Principale

Fabbrica d'Armi Pietro Beretta SpA  
Via Pietro Beretta, 18, Gardone Val Trompia, Brescia, Lombardy 25063, IT

Ottieni indicazioni



È possibile trovare anche informazioni riassuntive (e di partenza per future ricerche) riguardanti l'attuale presidente e CEO Franco Gussalli Beretta

**Franco Gussalli Beretta** · 2°

President & C.E.O. at Beretta | President at Confindustria Brescia | President at Sako OY | Executive Vice-President at Beretta Holding S.A. | Executive Vice-President at Beretta USA | President & C.E.O. at Norma USA

Parla di #education, #digitisation e #madeinbrescia

Brescia, Lombardia, Italia - [Informazioni di contatto](#)

29.035 follower · Più di 500 collegamenti

## Informazioni

Sono nato a Brescia nel 1964 ed assieme a mio fratello Pietro rappresento la 15^ generazione della famiglia Beretta, che dal 1526 è l'azionista di riferimento e guida la più antica fabbrica d'armi del mondo.

Dopo aver conseguito la laurea in Scienze Politiche presso l'università Carlo Bo di Urbino ed aver terminato il servizio militare nell'Arma dei Carabinieri, nel 1989 ho fatto il mio ingresso in Fabbrica d'Armi Pietro Beretta S.p.A. ricoprendo diversi ruoli fino a diventarmi Presidente nel maggio 2015. Nella mia carriera in azienda il primo incarico di responsabilità apicale mi venne dato nel 1997, quando mio padre nominò me Amministratore Delegato di Fabbrica d'Armi P.Beretta e mio fratello Amministratore Delegato della neonata Beretta Holding; al fine di operare al meglio nella gestione dei nuovi incarichi, il primo compito fu quello di scegliere il Direttore Generale.

All'interno del gruppo Beretta Holding ricopro attualmente i seguenti ruoli:

- Presidente & C.E.O. di Fabbrica d'Armi P.Beretta S.p.A.
- Executive Vice-President of Beretta Holding S.A.
- Executive Vice-President of Beretta USA Corp. (dal 1998)
- Presidente di SAKO OY (dal 2000)

Avendo l'onore e l'onere di portare avanti la pluricentenaria storia della mia famiglia, credo che la sfida più importante per la nostra generazione sia quella di guidare Beretta nella transizione digitale e sostenibile. Con questo importante obiettivo da raggiungere, sono costantemente impegnato nella gestione "industriale" delle aziende del gruppo, seguendo sempre la mia filosofia basata sul rispetto delle tradizioni ma seguendo sempre le innovazioni.

Ho visitato oltre 90 paesi in tutto il mondo, ma le mie radici sono sempre a Brescia, la città in cui vivo e per la quale amo dedicare il mio tempo e le mie forze. Dal 2021 ricopro l'incarico di Presidente di Confindustria Brescia e dal 2018 al 2021 il mio amore e la passione per i motori mi hanno portato alla Presidenza di Mille Miglia S.r.l., l'azienda in house dell'Automobile Club Brescia che organizza l'omonima gara e altre manifestazioni automobilistiche.

Sono sposato con Umberta ed abbiamo un figlio, Carlo, la 16^ generazione della famiglia. Attualmente faccio parte del Consiglio di Amministrazione delle aziende di famiglia di Umberta: HUG S.p.A., Almag S.p.A. e BRAWO S.p.A.

Le mie grandi passioni sono gli orologi, la nautica, le auto storiche e i viaggi.

Di lui sappiamo da articoli in rete che è sposato e ha un figlio, e ha svolto il servizio militare presso l'Arma dei Carabinieri.

## Franco Gussalli Beretta



Presidente della Fabbrica d'Armi Pietro Beretta S.p.A

Franco Gussalli Beretta, insieme al fratello Pietro, rappresenta la 15a generazione della famiglia. Sposato con Umberta Gnutti, un figlio, Carlo Alberto, studente universitario. Classe 1964, laureato in Scienze Politiche dopo aver completato il Liceo Scientifico. Servizio militare svolto nell'Arma dei Carabinieri. Dal 1996 è Amministratore Delegato di Fabbrica d'Armi Pietro Beretta SpA, di cui assume anche la presidenza nel 2015. Nel Gruppo di famiglia, ricopre anche le cariche di: Vice Presidente e Consigliere Delegato di Beretta Holding SpA, Executive Vice President di Beretta USA Corp., Presidente di SAKO OY, società finlandese produttrice di carabine ed è Consigliere di altre società del Gruppo. Oltre alle cariche ricoperte all'interno del Gruppo Beretta, è Consigliere d'Amministrazione di Almag e BRAVO, Presidente del Comitato Scientifico della Fondazione AIB e membro del Consiglio di Amministrazione di 1000 Miglia e Croce Bianca. Franco Gussalli Beretta dedica la maggior parte del suo tempo alle aziende industriali del Gruppo di famiglia, seguendo la filosofia di famiglia del rispetto della tradizione, ma con slancio verso l'innovazione e una parte del suo tempo a iniziative che reputa importanti per il territorio di Brescia.

La moglie Umberta Gnutti Gussa Beretta guida insieme a suo fratello Gabriele Gnutti il gruppo Gnutti, leader nel settore dell'ottone.

Il figlio Carlo Alberto Gussalli Beretta ha 26 anni e secondo le riviste è fidanzato con l'influencer Giulia De Lellis. Trattandosi di un lavoro pubblicamente esposto sarebbe utile monitorare l'andamento futuro nel caso in cui da dei post non controllati potessero trapelare informazioni personali di spessore.

Proseguendo la ricerca lancio da Kali il comando per rintracciare l'ip del sito beretta.com

```
(kali㉿Host-010)-[~]
$ nslookup www.beretta.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.beretta.com canonical name = 6tf64gx.impervadns.net.
Name:   6tf64gx.impervadns.net
Address: 45.60.65.151
```

Posso quindi cercare l'indirizzo IP su SHODAN, un motore di ricerca che permette agli utenti di trovare dispositivi connessi a Internet e vari servizi online. A differenza di motori di ricerca come Google che indicizzano i contenuti dei siti web, Shodan indicizza le informazioni relative ai servizi di rete, come i tipi di dispositivi connessi, se hanno porte aperte, quali servizi stanno eseguendo e altre informazioni tecniche.

Nello specifico, lo screenshot mostra le informazioni relative a un indirizzo IP (45.60.65.151), che sembra essere associato a Imperva Inc., una società di sicurezza informatica. Tra i dettagli abbiamo:

- General Information: Fornisce dettagli come il nome dell'host (imperva.com), il dominio (IMPERVA.COM), il paese (United States), la città (Redwood City), l'organizzazione e l'ISP (entrambi Incapsula Inc.), e l'ASN (Autonomous System Number) che è AS19551.
- Open Ports: Elenco delle porte aperte su quel dispositivo. Le porte aperte possono indicare quali servizi di rete sono accessibili dall'esterno. Per esempio, la porta 80 è comunemente usata per il traffico HTTP.
- Web Technologies: La sezione mostra le tecnologie web associate a quel dispositivo, in questo caso "Imperva".

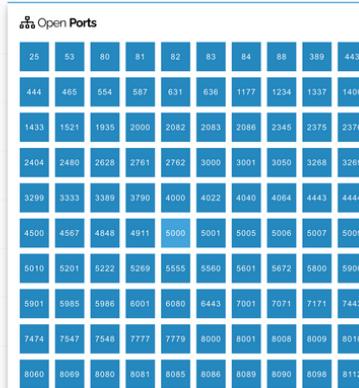
**General Information**

Hostnames	imperva.com
Domains	IMPERVA.COM
Country	United States
City	Redwood City
Organization	Incapsula Inc
ISP	Incapsula Inc
ASN	AS19551

**Web Technologies**

Security

Imperva



Su una delle porte aperte è visibile un estratto di un certificato SSL:

#### SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:  
01:9c:f4:91:65:6e:2f:35:80:a8:b2:3f:e7:b5:2b:b8

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2023 Q4

Validity

Not Before: Nov 7 17:44:49 2023 GMT

Not After : May 5 17:44:49 2024 GMT

Subject: CN=imperva.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:8d:22:cc:39:05:94:c9:d2:bd:57:dc:89:0f:aa:  
4c:62:1a:22:76:15:09:bf:f0:60:08:cb:22:d9:15:  
e0:f2:18:e7:18:4d:18:a8:e0:33:aa:71:c1:4e:c0:  
56:18:c2:37:92:21:9b:ce:42:b5:36:1b:cb:83:10:  
2c:93:a1:8a:8e:35:0b:26:bf:20:49:56:9b:89:a6:  
42:57:05:ae:0f:c3:ef:43:fa:a9:1e:70:2e:53:89:  
91:b1:33:ee:6d:66:0a:f9:a8:9e:75:23:23:59:b6:  
7a:d8:f5:7c:1b:cb:60:1f:b1:52:12:e8:e4:a5:52:  
50:52:d7:08:12:41:7a:01:2f:32:da:10:19:ae:3d:  
d8:9b:77:9f:d5:b5:96:59:07:bf:6d:4e:e4:d0:ab:  
cd:1f:b9:ad:88:87:67:48:c1:ce:8b:fb:50:af:65:  
c9:73:14:01:0d:72:42:ec:78:90:f8:e2:8c:26:6c:  
73:13:00:d2:ee:25:3b:6b:a1:8e:61:22:cf:cc:68:  
9a:ea:25:e6:84:3c:93:82:43:dd:d4:2e:76:da:60:  
3a:a8:2c:b9:35:bb:af:21:d1:c3:a9:cf:70:56:72:  
f3:a0:d5:00:fb:6f:2a:1c:18:1d:57:8d:1e:2a:6c:  
28:a5:26:8c:66:8f:b5:24:15:1b:4a:42:67:db:01:  
eb:d3

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Alternative Name:  
DNS:\*.beretta.com, DNS:\*.pietroberetta.com, DNS:imperva.com

X509v3 Key Usage: critical  
Digital Signature, Key Encipherment

- Versione, numero di serie e algoritmo di firma del certificato.
- L'emittente del certificato, che in questo caso è "GlobalSign nv-sa".
- La validità del certificato fino al 5 Maggio 2024.
- Il soggetto del certificato, che indica a chi è stato emesso il certificato (in questo caso, imperva.com).
- Informazioni sulla chiave pubblica, inclusi l'algoritmo e il modulo.
- Estensioni X509v3, che includono dettagli tecnici come l'uso della chiave, politiche di certificato e identificatori.
- L'indirizzo per l'accesso alle informazioni dell'autorità (AIA), che consente ai clienti di recuperare i certificati correlati per completare la catena di fiducia.
- La firma digitale del certificato, che assicura l'integrità del certificato e che non è stato manomesso.

I "Signed Certificate Timestamps" (SCT) sono associati alla Transparency Certificate e servono a fornire un sistema di registrazione pubblica dei certificati SSL, per prevenire l'emissione malevola di certificati.

Da terminale Kali prosegua lanciando il comando whois.

I dati mostrati includono diverse informazioni relative al dominio in questione. Tra queste:

- Domain Name: Il nome del dominio registrato.
- Registry Domain ID: Un identificativo unico per la registrazione del dominio nel sistema del registro.
- Registrar WHOIS Server: L'URL del server WHOIS del registratore, dove è possibile ottenere informazioni più dettagliate.
- Registrar URL: L'URL del registratore del dominio.
- Updated Date: L'ultima data in cui i dati del registro sono stati aggiornati.
- Creation Date: La data in cui il dominio è stato originariamente registrato.
- Registry Expiry Date: La data di scadenza della registrazione del dominio.
- Registrar: Il nome del registratore, che è l'organizzazione autorizzata a registrare il dominio.
- Registrar IANA ID: L'identificativo del registratore assegnato dalla Internet Assigned Numbers Authority (IANA).
- Registrar Abuse Contact Email e Phone: I contatti per segnalare eventuali abusi relativi al dominio.
- Domain Status: Mostra lo stato attuale del dominio secondo le specifiche ICANN (Internet Corporation for Assigned Names and Numbers). "clientTransferProhibited" significa che il dominio non può essere trasferito a un altro registratore senza l'autorizzazione del proprietario del dominio.
- Name Servers: I server dei nomi (DNS) attualmente impostati per il dominio, che indirizzano dove vengono gestite le richieste per il dominio.
- Registrant Phone/Fax/Email: Questi sono i contatti telefonici, del fax e l'email del registrante del dominio, ovvero la persona o l'organizzazione che possiede il dominio.
- Registry Registrant/Admin ID: L'identificativo unico dell'amministratore del registro per questo dominio: Gussalli Beretta Franco
- Admin Name/Organization/Address: Informazioni dettagliate sull'amministratore del dominio, incluso il nome, l'organizzazione (Fabbrica d'Armi Pietro Beretta S.p.A.), e l'indirizzo fisico.
- Admin Country/Phone/Fax/Email: Ulteriori informazioni di contatto per l'amministratore, inclusi paese, telefono, fax, e email.
- Registry Tech ID: L'identificativo unico del contatto tecnico per questo dominio.
- Tech Name/Organization/Address: Informazioni simili a quelle dell'amministratore, ma per il contatto tecnico del dominio, che in questo caso è Matteo Lombardi di Defende Sas di Matteo Lombardi.
- Tech Country/Phone/Fax/Email: Contatti telefonici, del fax, e l'email del contatto tecnico.

- Name Servers: I server dei nomi assegnati al dominio, che gestiscono la risoluzione dei nomi di dominio in indirizzi IP.
- DNSSEC: Stato della sicurezza del sistema dei nomi di dominio (DNS Security Extensions). "unsigned" significa che per questo dominio non è attualmente utilizzata la firma digitale per aumentare la sicurezza.
- URL of the ICANN Whois Inaccuracy Complaint Form: Un link per segnalare all'ICANN eventuali inesattezze nelle informazioni WHOIS.

```

File Actions Edit View Help
[~] kali@Host-010: ~
# whois beretta.com
Domain Name: BERETTA.COM
Registry Domain ID: 2549815_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.EuroDNS.com
Updated Date: 2023-08-29T15:38:57Z
Creation Date: 1997-03-18T05:00:00Z
Registry Expiry Date: 2024-03-19T04:00:00Z
Registrar: EuroDNS S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.WRONS.IT
Name Server: NS2.WRONS.IT
Name Server: NS3.WRONS.IT
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-12-19T21:38:17Z <<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE! The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services ("VeriSign") Whois database is provided "as-is" for
information purposes only, and is not intended to assist persons in obtaining
information about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems); The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database and its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrants.
Domain Name: beretta.com
Registry Domain ID: 028729916-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2023-08-29T17:38:59Z
Creation Date: 1997-03-18T00:00:00Z
Registrar Registration Expiration Date: 2024-03-18T00:00:00Z
Registrar: EuroDNS S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Gussalli Beretta Franco
Registrant Organization: Fabbrica d'Armi Pietro Beretta S.p.A.
Registrant Street: Via P. Beretta 18
Registrant City: Gardone Val Trompia
Registrant State/Province:
Registrant Postal Code: 25063
Registrant Country: IT
Registrant Phone: +39.372880740
Registrant Email:
Registrant Admin ID:
Admin Name: Gussalli Beretta Franco
Admin Organization: Fabbrica d'Armi Pietro Beretta S.p.A.,
Admin Street: Via P. Beretta 18
Admin City: Gardone Val Trompia
Admin State/Province:
Admin Postal Code: 25063
Admin Country: IT
Admin Phone: +39.372880740
Admin Fax:
Admin Email: domain@defende.it
Registrant Tech ID:
Tech Name: Lombardi Matteo
Tech Organization: Defende Sas di Matteo Lombardi
Tech Street: Via Persico, 31
Tech City: Cremona
Tech State/Province:
Tech Postal Code: 26100
Tech Country: IT
Tech Phone: +39.372880740
Tech Fax: +39.372880742
Tech Email: matteo.lombardi@defende.it
Name Server: ns1.wronds.it
Name Server: ns2.wronds.it
Name Server: ns3.wronds.it
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-12-19T21:38:17Z <<
For more information on Whois status codes, please visit https://icann.org/epp

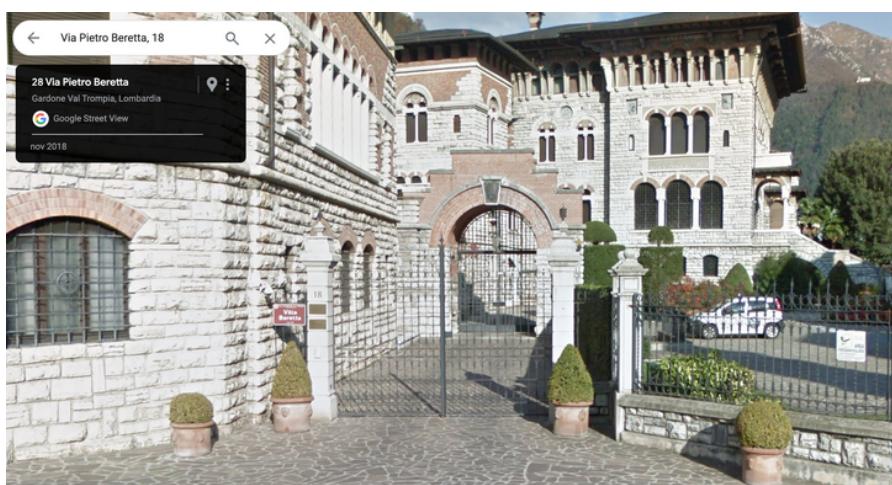
Please email the listed admin email address if you wish to raise a legal issue.

The Data in EuroDNS WHOIS database is provided for information purposes only.
The fact that EuroDNS display such information does not provide any guarantee
about the accuracy on the purpose for which the database may be used, its
accuracy or usefulness. By submitting a WHOIS query, you agree that you will
use this Data only for lawful purposes and that, under no circumstances will
you use this Data to:
(1) allow, enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via e-mail (spam); or
(2) enable high volume, automated, electronic processes that apply to EuroDNS
(or its systems). EuroDNS reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by the above policy.

```

In basso vista della via legata  
all'amministratore del registro del dominio.

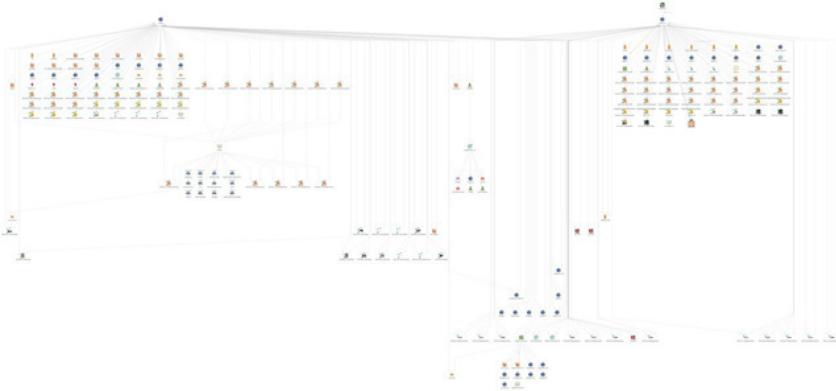


## Maltego

Maltego è uno strumento utilizzato principalmente per l'analisi forense digitale e l'intelligence open source (OSINT). È progettato per raccogliere e analizzare grandi quantità di informazioni provenienti da diverse fonti, permettendo agli utenti di visualizzare le connessioni tra i dati in maniera intuitiva.

Alcuni usi:

1. Analisi di Rete e Sicurezza Informatica: Maltego è ampiamente utilizzato per identificare vulnerabilità e minacce in reti informatiche. Può aiutare a scoprire relazioni nascoste tra vari nodi in una rete, come server, domini e indirizzi IP.
2. Raccolta di Informazioni in OSINT: Gli investigatori utilizzano Maltego per raccogliere informazioni da fonti pubbliche. È utile per raccogliere dati da social media, database pubblici, siti web, e altre fonti online accessibili al pubblico.
3. Analisi Forense: Nelle indagini digitali, Maltego può essere utilizzato per tracciare l'attività criminale e scoprire relazioni tra diversi elementi di un caso, come individui, organizzazioni, e transazioni.
4. Ricerca sulle Minacce e Analisi del Cybercrime: Gli analisti di sicurezza possono utilizzare Maltego per identificare e analizzare campagne di cybercrime, tracciare attori di minaccia e comprendere meglio la natura delle attività malevoli.
5. Gestione dell'Identità e dell'Accesso: Maltego può essere impiegato per analizzare e visualizzare le relazioni tra identità digitali, aiutando a gestire l'accesso e la sicurezza delle informazioni.
6. Analisi di Mercato e Competitive Intelligence: In ambito aziendale, Maltego può essere utilizzato per raccogliere e analizzare informazioni sui concorrenti, sul mercato e sulle tendenze del settore.



Nell'esercizio di oggi Maltego è stato utile per molteplici motivi. In particolare l'ho trovato utile per comprendere meglio le relazioni tra i vari domini e sottodomini e per avere una chiara visuale della struttura e "storia" del sito target.

Oltre ai vari dati di ip, host, etc.. già precedentemente ricavati usando altri tool si notano ad esempio dei collegamenti con l'azienda americana americaneagle.com. Andando ad approfondire sul loro sito comprendiamo che si è occupata del redesign e dello sviluppo del sito Beretta USA per renderlo più moderno e appetibile sul mercato americano. Per collezionare ulteriori informazioni di contatto sui lavoratori dell'americaneagle.com che

potrebbero aver lavorato sul sito di Beretta ho cercato da terminale:

```
[recon-ng][default][whois_pocs] > options set SOURCE americanaeagle.com
SOURCE => americanaeagle.com
[recon-ng][default][whois_pocs] > run
```

---

AMERICANEAGLE.COM

Overview

[+] URL: http://whois.arin.net/rest/pocs?domain=americanaeagle.com  
[+] URL: http://whois.arin.net/rest/poc/CH084-ARIN  
[+] Country: United States  
[+] Email: chris@americanaeagle.com  
[+] First\_Name: Chris  
[+] Last\_Name: Hollenbeck  
[+] Middle\_Name: None  
[+] Notes: None  
[+] Phone: None  
[+] Region: Park Ridge, IL  
[+] Title: Whois contact  
[+]  
[+] URL: http://whois.arin.net/rest/poc/KIERZ12-ARIN  
[+] Country: United States  
[+] Email: markk@americanaeagle.com  
[+] First\_Name: MARK  
[+] Last\_Name: KIERZKOWSKI  
[+] Middle\_Name: None  
[+] Notes: None  
[+] Phone: None  
[+] Region: Chicago, IL  
[+] Title: Whois contact  
[+]  
[+] URL: http://whois.arin.net/rest/poc/KIERZ13-ARIN  
[+] Country: United States  
[+] Email: markk@americanaeagle.com  
[+] First\_Name: MARK  
[+] Last\_Name: KIERZKOWSKI  
[+] Middle\_Name: None  
[+] Notes: None  
[+] Phone: None  
[+] Region: Chicago, IL  
[+] Title: Whois contact  
[+]  
[+] URL: http://whois.arin.net/rest/poc/KIERZ18-ARIN  
[+] Country: United States  
[+] Email: markk@americanaeagle.com  
[+] First\_Name: Mark  
[+] Last\_Name: Kierzkowski  
[+] Middle\_Name: None  
[+] Notes: None

Detail View

Relationships

Generator detail

Source

Transform

Gen. date

Properties

Domain Name

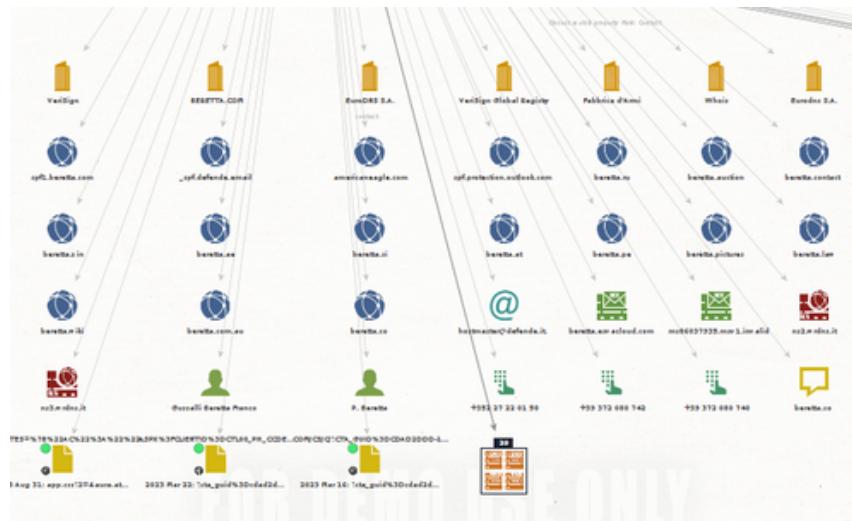
Dynamic properties

Notes

Graph Info

Comments

Hub



Tra i contatti diretti al sito beretta.com compaiono Franco Gussalli Beretta e P.Beretta oltre a diverse mail di dipendenti di società operanti nel settore dello sviluppo web e della cyber security. Ad esempio espandendo P. Beretta notiamo il collegamento con Santosh Raghavan di Seranova, azienda operante nel settore tech.

