

Esercizio S5L2

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

Alla fine dell'analisi, lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato:

- Il target
- Le query utilizzate (dove applicabile)
- I risultati ottenuti

L'esercizio chiedeva di raccogliere dell'informazioni su di me(1) e sul dominio di Eicode(2), grazie a degli strumenti(Google e Maltego) e come risultati mostrati qui sotto:

Maltego 1

FOR DEMO USE ONLY

Per quanto riguarda la ricerca su me non vi è nessun risultato su Maltego come mostrato la figura a sinistra.

Google 1

Duc Tin Ly - Veneto, Italia | Profilo professionale

Duc Tin Ly - Stagista presso Martini S.r.l. - Visualizza i collegamenti in comune con Duc Tin - Piacere di rivederti - Esperienza - Altre persone che si chiamano Duc ...

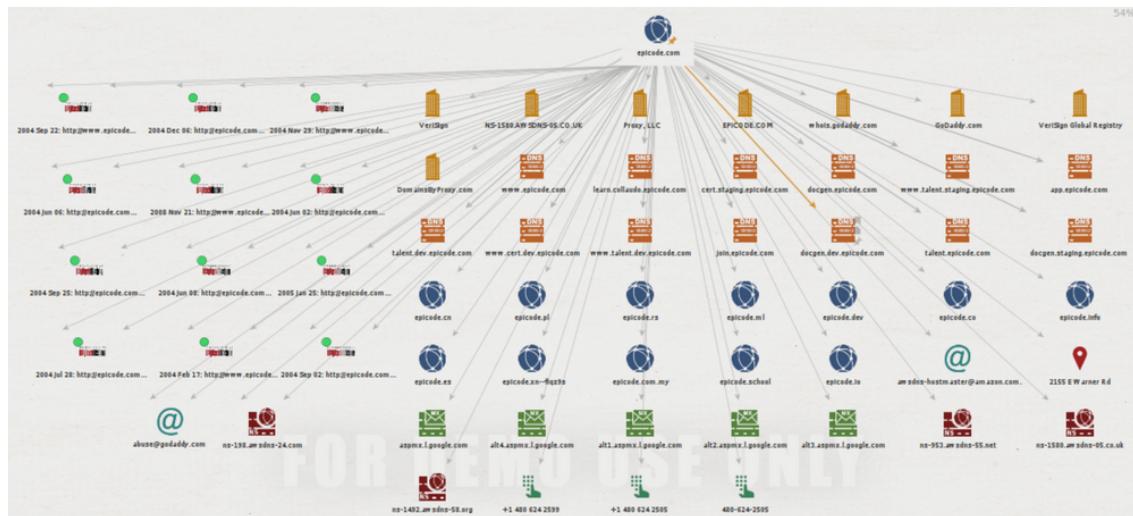
Facebook

https://m.facebook.com/ducitin - Traduci questa pagina

Duc Tin Ly | فيسبوك

Duc Tin Ly موجود على فيسبوك. أنت إلى قيسنوك للتواصل مع Duc Tin Ly وأصحاب آخرين في Duc Tin Ly. تعرفهم، يفتح قيسنوك الأشخاص المقدرة على المشاركة، وجعل العالم ...

Invece su Google vi è soltanto un risultato.



Per quanto riguarda Eicode come mostrato nell'immagini a sinistra si può vedere le sedi, dei server DNS, dei numeri di telefono, dell'e-mail server, dei altri sottodomini, dell'e-mail e dei siti di wayback machine che mostrano in vari anni il progresso del dominio.

 EPICODE
<https://epicode.com> ...

EPICODE - Sblocca competenze tech e inizia subito a lavorare

Con **Epicode** studi 100% online, diventi professionista e vai a lavorare per le aziende più influenti al mondo. Paghi solo quando trovi lavoro.

Tutti i corsi
Il metodo didattico EPICODE. Un corso di programmazione ...

Corso Full-Stack Developer
Corso web developer da zero: in 6 mesi diventi sviluppatore web e ...

Metodi di pagamento
Epicode quanto costa ; Corsi Full-Time 6 mesi. Corso Full-Stack ...

Corso Cybersecurity
Correggi e valuta il lavoro della giornata. Il metodo didattico ...

[Altri risultati in epicode.com »](#)



EPICODE

Visualizza foto

Guarda esterni

EPICODE

Sito web Indicazioni Salva

Centro di formazione a Roma

Indirizzo: Via dei Magazzini Generali, 16, 00154 Roma RM

Orari: Chiude tra poco · 18:30 · Apre mer alle ore 09 ·

Telefono: 351 779 6872

Su Google vi sono risultati del sito di Epicode e anche in altri siti dove Epicode si è registrato.

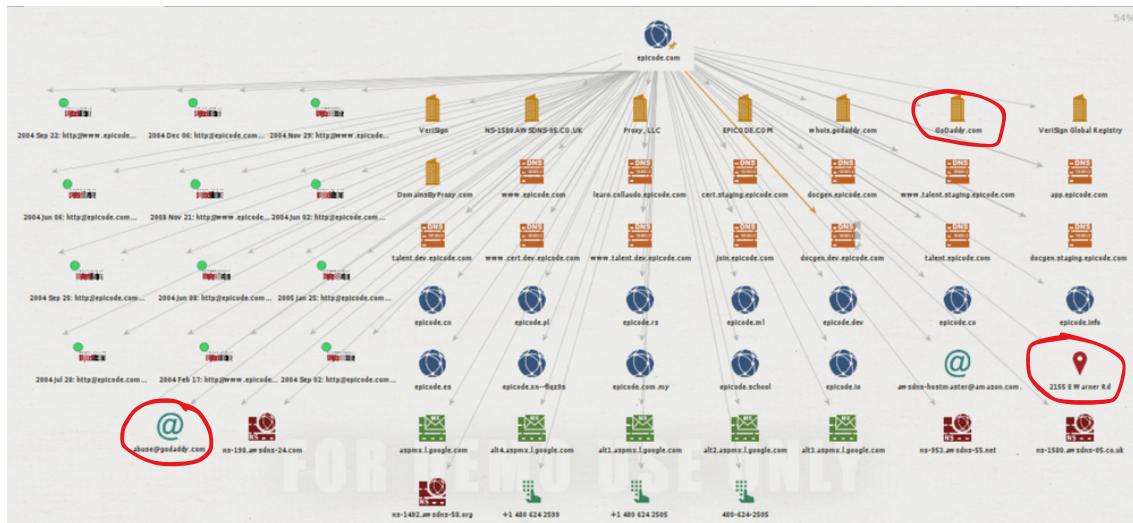
Da qui mostra il luogo della sede, gli orari, un numero di cellulare di contatto.

Sito ufficiale di EpiCode

Si può vedere che il sito offre un'istruzione nell'ambito dell'informatica.

Sito ufficiale di Episode del 2004

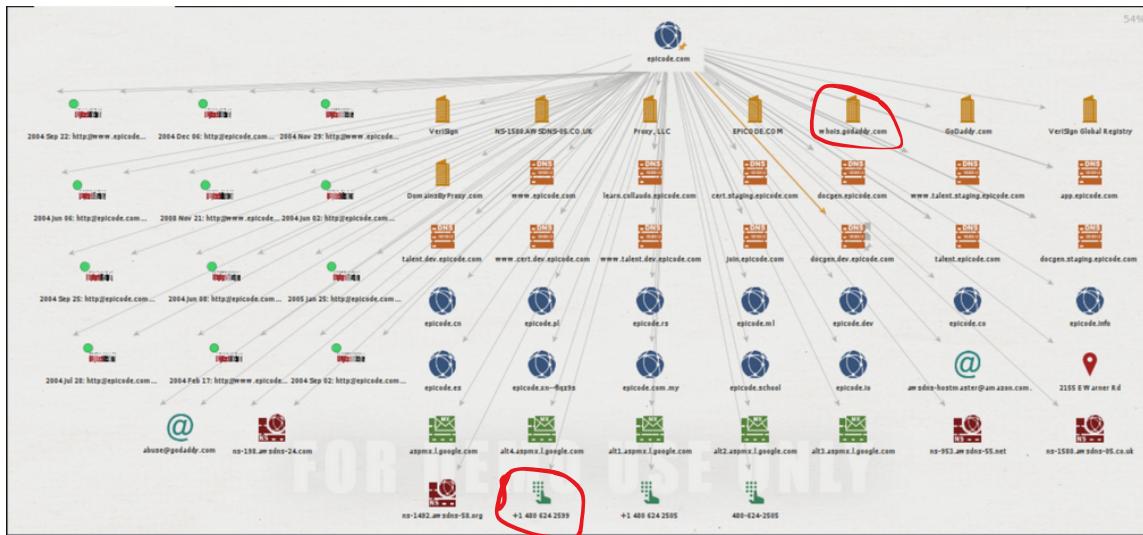
Invece qui vende dei software per la modellazione della dispersione chimica



Il dominio GoDaddy è un'azienda che fornisce hosting e registrazione di domini internet tra cui, si suppone, anche quello di Epicode

sito ufficiale di GoDaddy

Mostra la sede del sito GoDaddy che si trova in America



Dal sito di Whois si può ricavare ulteriori informazioni a riguardo del sito GoDaddy, da lì vi è un numero di telefono che corrisponde al numero cerchiato.

Come mostrato nell'immagine sopra, si può ottenere dell'informazioni fondamentali che rende l'azienda vulnerabile a possibili attacchi



Verysign un'altro sito simile a Whois che serve per ottenere altri informazioni del dominio che si vuole riguardante alla rete dell'azienda

Whoisgodaddy.com

AS20362 VeriSign Global

AS20362 – VeriSign Global Registry Services

IP Range	Company	Size of IP
102.32.56.0/24	VeriSign Global Registry Services	256
102.32.247.0/24	VeriSign Global Registry Services	256
102.32.52.0/24	VeriSign Global Registry Services	256
102.32.45.0/24	VeriSign Global Registry Services	256
102.32.80.0/24	VeriSign Global Registry Services	256
102.32.173.0/24	VeriSign Global Registry Services	256
102.42.75.0/24	VeriSign Global Registry Services	256
102.42.177.0/24	VeriSign Global Registry Services	256
102.3.5.0/24	VeriSign Global Registry Services	256
102.18.130.0/24	VeriSign Global Registry Services	256

WHOIS Details

 <https://www.verisign.com> · Traduci questa pagina

Verisign is a global provider of domain name registry services ...

Verisign enables the world to connect online with reliability and confidence - anytime, anywhere.

- A leader in domain name registry services and internet ...

Domain Names

Domain Name Search - Find a Registrar - Become A Registrar

Search Whois

Verisign's Whois tool allows users to look up records in the registry ...

Company Information

Verisign's critical yet mostly invisible role – helping to ...

Careers

Verisign is committed to providing resources to manage a healthy ...

Altri risultati in verisign.com »

 <https://it.wikipedia.org/wiki/Verisign>

Verisign

Verisign, Inc. (stilizzato in **VERISIGN**) (NASDAQ: **VRSN**) è una società statunitense con sede a Reston, in Virginia, che gestisce un'ampia gamma di ...

Storia - Prodotti e servizi - Note

Verisign: Il Sigillo Sito Sicuro

 [Verisign](#) 

VeriSign, Inc. è una società statunitense con sede a Reston, in Virginia, che gestisce un'ampia gamma di infrastrutture di Rete, fra cui due dei treddici server dei nomi radice operanti in Internet. Il ... [Wikipedia](#)

Valore azionario: **VRSN** (NASDAQ)
192,63 USD -11,90 (-5,82%)
27/08/16 00:00 GMT-4 - Limitazione di responsabilità

CEO: [James Bidzos](#) (ago 2011-)

Sede centrale: Reston, Virginia, Stati Uniti

Consociate: Jamba, LightSurf, Domainnames.com

Limited, ALTRO

Fondatore: [James Bidzos](#)

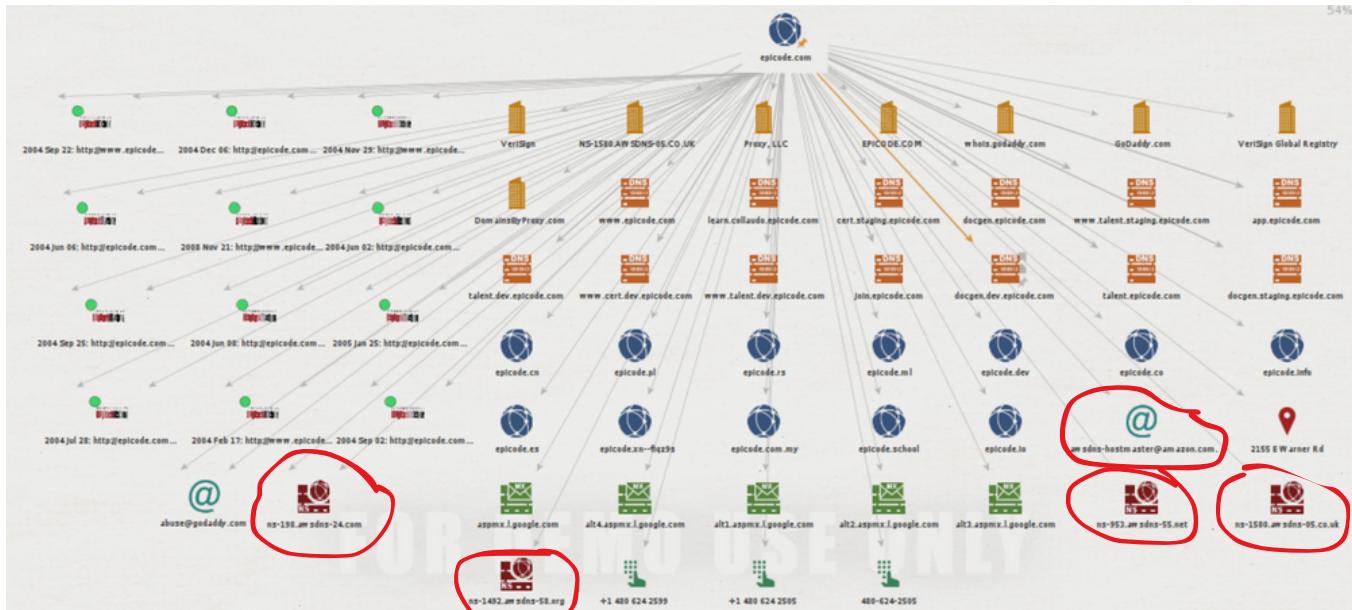
Fondazione: aprile 1995

[Limitazione di responsabilità](#)

Profili

 [LinkedIn](#)  [Twitter](#)  [Facebook](#)

Verysign è una società che gestisce un'ampia gamma di infrastrutture di Rete, fra cui due dei tredici server dei nomi radice operanti in Internet, il registro con autorità per i Domini di primo livello generici .com, .net e .name, nonché per i domini di primo livello con codice paese .cc e .tv e i sistemi di back-end per i domini di primo livello .jobs e .edu. Inoltre offre tutta una serie di servizi di sicurezza, quali amministrazione di DNS, Distributed Denial of Service (DDoS) e monitoraggio di minacce informatiche.



aws.amazon.com
https://aws.amazon.com/account/sign-up

Amazon Web Services | Inizia A Innovare Su AWS

Registri E Prova I Servizi Sicuri, Affidabili E Scalabili Di AWS. Crea, Implementa E Gestisci Siti Web, App O Processi.

Cloud computing
Amazon S3 - Archiviazione durevole e scalabile.

Elaborazione AWS Cloud
AWS Lightsail: servizi di elaborazione di semplice utilizzo.

Soluzioni AWS Storage
Amazon S3 offre un servizio di archiviazione scalabile.

Current AWS Customers
Get the Most Out of AWS Cloud. Pick a Learning Path & Get Started.

Amazon Web Services
https://aws.amazon.com/ ...

Servizi di cloud computing – Amazon Web Services (AWS)

Amazon Web Services offre servizi di cloud computing affidabili, scalabili ed economici. L'account è gratuito e si pagano solo i servizi usati.

Piano gratuito di AWS

Amazon Web Services

Azienda

Amazon Web Services, Inc. è un'azienda statunitense di proprietà del gruppo Amazon, che fornisce servizi di cloud computing su un'omonima piattaforma on demand. Questi servizi sono operativi in 26 regioni geografiche in cui Amazon stessa ha suddiviso il globo, più altre 8 regioni disponibili prossimamente. Wikipedia

CEO: Adam Selipsky (17 mag 2021–)

Fondazione: marzo 2006

Sede centrale: Seattle, Washington, Stati Uniti

Fondatore: Amazon.it

Organizzazione principale: Amazon.it

Consociate: CloudEndure, Elemental Technologies, Inc., Wickr, ALTRO

Gruppo: Amazon

Limitazione di responsabilità

aws - Cerca con Google

https://aws.amazon.com/it/free/?trk=b16dcdbd-9bf8-4a7b-9d68-04b5a8b8914&sc_channel=ps&ef_id=ElAaQ...

Dettagli

Summary Attachments (0) Notes Properties (1)

awsdns-hostmaster@amazon.com.

Email Address

Google Mel Wikipedia Mel

Servizi di cloud computing – Amazon Web Services (AWS)

Amazon Web Services offre servizi di cloud computing affidabili, scalabili ed economici. L'account è gratuito e si pagano solo i servizi usati.

Piano gratuito di AWS

Panoramico Categorie del piano gratuito Come creare un account Offerte in evidenza per le aziende Domande frequenti Termini e condizioni

Esplora le principali categorie di prodotti

Dettagli del piano gratuito

Filtra per:

CANCELLA TUTTI I FILTRI

Tipo di piano

In evidenza

Gratuito per 12 mesi

Gratuito senza limiti di tempo

Prove gratuite

Categorie di prodotti

Analisi dei dati

CALCOLO **ARCHIVIAZIONE** **DATABASE**

Piano gratuito GRATIS PER 12 MESI

Amazon EC2 **750 ore**

5 GB al mese

Capacità di elaborazione

Amazon S3 **5 GB**

5 GB storage standard

Infrastruttura di storage di oggetti

Amazon RDS **750 ore**

50 ore di utilizzo del database (motori di database applicabili)

Summary Attachments (0) Notes Properties (1)

ns-198.awsdns-24.com

NS Record

DNS records for ns-1492...

ns-198.Awsdns-24.Com

Google Mel Wikipedia Mel

MYIP.MS

Hosting Info, Websites & IP Database

Enter Website or IPv4/IPv6 (2.1.7.5, yahoo.com) or any search text

Products Hosting Companies Websites Blacklist / IP Database Interesting Sitemap API

Home IP Websites Sites DNS (Nameservers) ns-198.awsdns-24.com - USA

Where Information on this Nameserver

Nameserver (DNS) ns-198.awsdns-24.com

Nameserver IP Address: 209.251.192.198

Nameserver IPv6 Address: 2600:9000:300:c600:1

Country: USA

Update Time: 01 Nov 2023, 16:42

Total Websites using Nameserver: 863 sites

TOP World Websites using Nameserver (from World Top 100,000 sites): 21 sites

Indirizzo IP pubblico Amazon

aws - Cerca con Google

https://www.nslookup.io/domains/ns-1492.awsdns-58.org/dns-records/

Dettagli

Summary Attachments (0) Notes Properties (1)

ns-198.awsdns-24.com

NS Record

DNS records for ns-1492...

ns-198.Awsdns-24.Com

Google Mel Wikipedia Mel

Cloudflare

Cloudflare Google DNS OpenDNS Authoritative Local DNS

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address: 205.251.192.212 Revalidate in: 48h

AAAA records

IPv6 address: 2600:9000:5305:d400:1 Revalidate in: 48h

CNAME record

No CNAME record found.

TXT records

No TXT records found.

List of websites using nameserver: ns-198.awsdns-24.com

No	Web Site	Website IP Address	Web Hosting Company / IP Owner	Web Hosting / Server IP Location	Web Hosting City	World Site Popular Rating
1	tradingeconomics.com	3.221.244.255	Amazon.com, Inc	USA	Plano	# 1,351
2	spiceworks.com	45.60.11.212	Incapsula Inc	USA		# 2,537
3	ustraveldocs.com	52.84.90.10	Amazon.com, Inc	USA		# 3,292
4	nicochannel.jp	13.224.132.79	Amazon.com, Inc	USA		# 14,539
5	iphone-mania.jp	52.84.90.19	Amazon.com, Inc	USA		# 27,199
6	takeshobo.co.jp	13.113.108.207	Amazon.com, Inc	Japan	Tokyo	# 27,469
7	mqn.jp	143.204.68.27	Amazon.com, Inc	USA		# 34,064
8	techreviewer.com	18.164.68.17	Amazon.com, Inc	USA		# 38,213
9	garbarino.com	3.222.253.113	Amazon.com, Inc	USA		# 40,469
10	hololive-ic.com	143.204.176.32	Amazon.com, Inc	USA		# 49,526

Indirizzo IP e nome di dominio dei siti correlati ad Amazon

aws - Cerca con Google

https://myip.ms/view/dns/44986/ns-198.awsdns-24.com

Dettagli

Summary Attachments (0) Notes Properties (1)

ns-198.awsdns-24.com

NS Record

DNS records for ns-1492...

ns-198.Awsdns-24.Com

Google Mel Wikipedia Mel

MYIP.MS

Hosting Info, Websites & IP Database

Enter Website or IPv4/IPv6 (2.1.7.5, yahoo.com) or any search text

Products Hosting Companies Websites Blacklist / IP Database Interesting Sitemap API

Home IP Websites Sites DNS (Nameservers) ns-198.awsdns-24.com - USA

Where Information on this Nameserver

Nameserver (DNS) ns-198.awsdns-24.com

Nameserver IP Address: 209.251.192.198

Nameserver IPv6 Address: 2600:9000:300:c600:1

Country: USA

Update Time: 01 Nov 2023, 16:42

Total Websites using Nameserver: 863 sites

TOP World Websites using Nameserver (from World Top 100,000 sites): 21 sites

List of websites using nameserver: ns-198.awsdns-24.com

No	Web Site	Website IP Address	Web Hosting Company / IP Owner	Web Hosting / Server IP Location	Web Hosting City	World Site Popular Rating
1	tradingeconomics.com	3.221.244.255	Amazon.com, Inc	USA	Plano	# 1,351
2	spiceworks.com	45.60.11.212	Incapsula Inc	USA		# 2,537
3	ustraveldocs.com	52.84.90.10	Amazon.com, Inc	USA		# 3,292
4	nicochannel.jp	13.224.132.79	Amazon.com, Inc	USA		# 14,539
5	iphone-mania.jp	52.84.90.19	Amazon.com, Inc	USA		# 27,199
6	takeshobo.co.jp	13.113.108.207	Amazon.com, Inc	Japan	Tokyo	# 27,469
7	mqn.jp	143.204.68.27	Amazon.com, Inc	USA		# 34,064
8	techreviewer.com	18.164.68.17	Amazon.com, Inc	USA		# 38,213
9	garbarino.com	3.222.253.113	Amazon.com, Inc	USA		# 40,469
10	hololive-ic.com	143.204.176.32	Amazon.com, Inc	USA		# 49,526

mappa totale correlato ad Epicode

