



CYBERSECURITY
NATIONAL LAB

CYBER
HIGH
SCHOOLS



SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

1st HighSchools CTF Workshop

Open Source Intelligence

ITASEC23

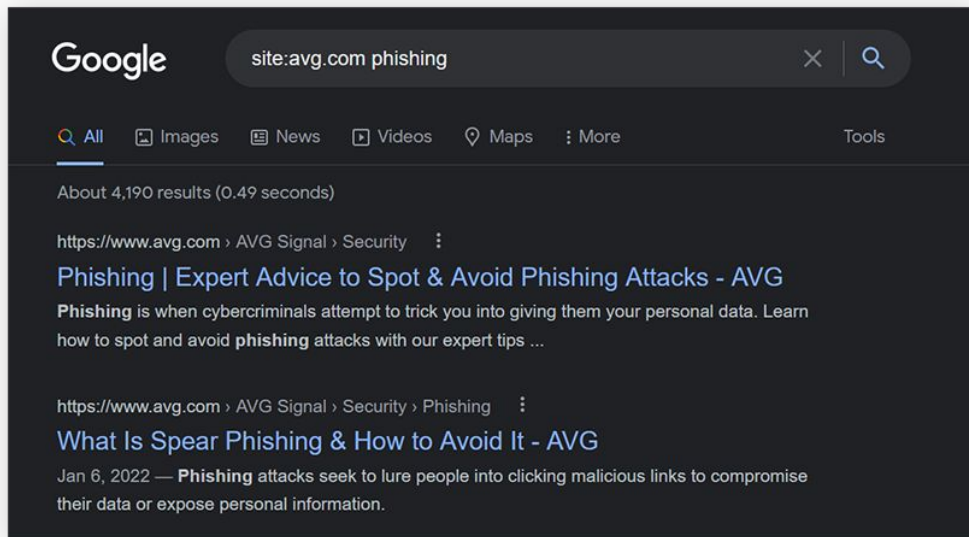
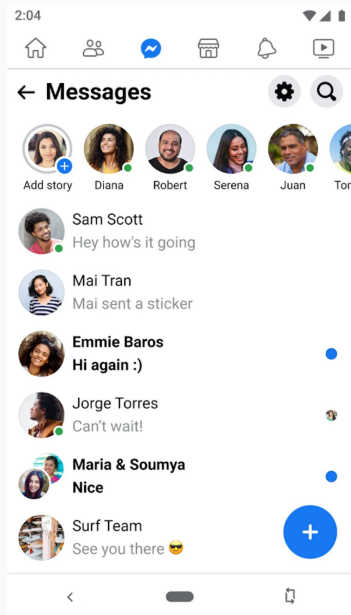
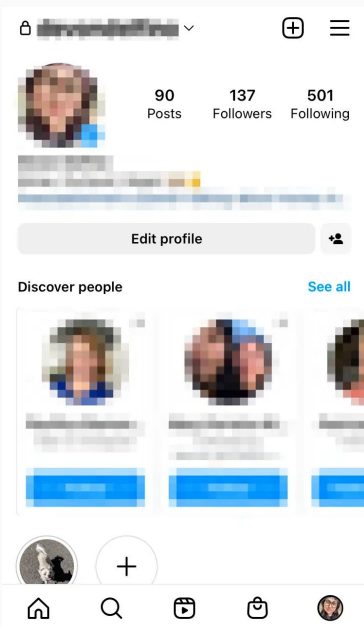
ITALIAN CONFERENCE ON CYBERSECURITY

May 2nd-5th, 2023 - Bari

Oscar Urselli - Politecnico di Bari
Pierluigi De Palo - Università di Bari

Che cos'è l'OSINT?

L'Open Source Intelligence (**OSINT**) è una tecnica di raccolta dati, tramite risorse **pubblicamente accessibili** quali ad esempio social networks o siti web



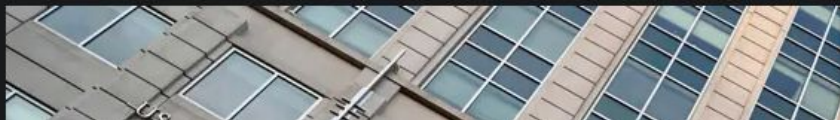
Che cos'è l'OSINT?

Contrariamente a quanto si possa pensare, per ottenere dati sensibili, non è necessario infiltrarsi in un sistema.

Perché spesso i dati sono già disponibili online...

Ice inadvertently posted personal information of 6,252 people in custody

Worry after agency spreadsheet was erroneously posted online 'while performing routine updates' and was up for about five hours



CBC

MENU

NEWS

Top Stories

Local

Climate

World

Canada

Politics

In

Politics

Green Party posted sensitive information about voters and members online

A che cosa serve?

Le informazioni raccolte, grazie all'**OSINT**, possono essere utilizzate per scopi legali come:

- rintracciare un fuggitivo o una persona scomparsa
- condurre le indagini e scoprire il colpevole di un reato
- individuare i punti deboli di un'azienda che un attaccante potrebbe sfruttare

Però, questi dati, sono disponibili anche a criminali che potrebbero voler:

- fare phishing
- ottenere dati sensibili
- rubare l'identità di una persona

Information gathering

Google Dorks

- Sono i “comandi” di Google;
- Permettono di trovare informazioni che sarebbero inaccessibili con una ricerca normale;
- Tornano quindi utili sia in scenari di attacco, sia di difesa.

Dorks cheatsheet

Operatore	Funzione	Esempio
site:	Ritorna una lista di tutti gli URL indicizzati del sito specificato	site:medium.com
ext:	Ritorna i file con una certa estensione	ext:pdf
intext:	Ritorna le pagine che contengono una certa stringa	intext:"ITASEC"
inurl:	Ritorna gli URL contenenti una certa stringa	inurl:blog

Altri dorks: <https://bit.ly/3UW2n89>

Google Dorks: Alcuni esempi

site:medium.com

Google Search Console
www.google.com/webmasters/
Do you own **medium.com**? Get indexing and ranking data from Google.

medium.com
https://medium.com

Medium – Where good ideas find you.
Medium is an open platform where readers find dynamic thinking, and where expert and undiscovered voices can share their writing on any topic.

medium.com
https://caityjohnstone.medium.com

Caitlin Johnstone – Medium
Read writing from Caitlin Johnstone on Medium. I write about the end of illusions. Every day, Caitlin Johnstone and thousands of other voices read, write, ...

medium.com
https://youssefraaat57.medium.com

Youssef Hosni – Medium
Read writing from Youssef Hosni on Medium. Computer Vision Researcher | Data Scientist | I Write to Understand | Looking for data science mentoring, ...

medium.com
https://kokumura.medium.com

Kaki Okumura – Medium
Read writing from Kaki Okumura on Medium. Born in Dallas, raised in New York and Tokyo. I care about helping others learn to live a better, healthier life.

site:medium.com ext.pdf

About 161 results (0.19 seconds)

medium.com
https://medium.com › media › href PDF

Junya Ishigami - cloudfont.net
Jun 16, 2013 — Dit kijken naar de planeet, dit 'kosmisch' perspectief op de natuur weet. Ishigami met brio om te zetten in bouwwerken die op verschillende.

medium.com
https://link.medium.com › ... PDF

Critical theory in The Empire of Sheep, a review by ...
"We're living in a world that's upside down. Where the exception has become the rule. Where the margins have become king. The aesthetics of the carnival are ...

medium.com
https://medium.com › media › href PDF

Dossiê Mulher 2017
by AS Pinto · 2017 · Cited by 2 — Equipe. Afonso Borges. Aloísio Geraldo Sabino Lopes. Bárbara Caballero. Caio de Almeida. Débora Souza. Diego Gimenes.

medium.com
https://medium.com › media › href PDF

(English Translation Below) 株式会社 みずほフィナンシャル ...
地球温暖化の大きな原因である化石燃料の中で、最もCO2排出量が多いのが石炭です。石炭、採掘の際に環境破壊や水資源汚染を引き起こし、発電の際には大気汚染に ...

medium.com
https://medium.com › media › href PDF

Trends in State Tax Policy, 2018
Dec 4, 2017 — State tax changes are not made in a vacuum. States often adopt policies after watching peers address similar issues.

Google Dorks: Alcuni esempi

site:medium.com intext:"ITASEC"

About 37 results (0.29 seconds)

medium.com
https://medium.com › innovaetica › research-proof-at-...
Research Proof at Itasec 2019 - by Innovaetica S.r.l.
May 8, 2019 — The Italian Conference on CyberSecurity (ITASEC) is an annual event supported and organized by the Cybersecurity National Lab. www.itasec.it.

medium.com
https://medium.com › innovaetica
Innovaetica
Leading experts in blockchain and cryptographic technologies · Research Proof at Comdirect & Partners Corporate Day · Research Proof at **Itasec** 2019 · What is ...

medium.com
https://medium.com › researchproof
ResearchProof
Mar 17, 2020 — Research Proof at **Itasec** 2019. Recently, we presented the ResearchProof Registry at **ITASEC**, the main Italian Conference on Cybersecurity, which ...

medium.com
https://medium.com › ...
ResearchProof
Recently, we presented the ResearchProof Registry at **ITASEC**, the main Italian Conference on Cybersecurity, which was held in Pisa between the 12th and the 15th ...

medium.com
https://medium.com › innovaetica › trending
Trending stories published on Innovaetica
Research Proof at **Itasec** 2019 ... Recently, we presented the ResearchProof Registry at **ITASEC**, the main Italian Conference on Cybersecurity... Read more...

site:medium.com inurl:"blog"

About 362,000 results (0.38 seconds)

medium.com
https://medium.com › angular-blog
Angular Blog
The latest news and tips from the Angular team.

medium.com
https://blog.medium.com
The Official Medium Blog | News, Updates, and Tips
3 Min Read is the official Medium blog. Stay up to date on the latest features, news, and writing advice from Medium. For readers and writers on Medium.

medium.com
https://medium.com › trezor-security-blog
Trezor Blog
The official blog for the world's first hardware wallet — Trezor. All you need to keep your bitcoin and digital identity safe.

medium.com
https://medium.com › empatica-blog
Blog | Empatica
The Empatica Health Monitoring Platform receives FDA-clearance ; NewsResearch · Measuring the stress levels of an Analog Space Mission crew using EmbracePlus.

medium.com
https://medium.com › viki-blog
Viki Blog - Rakuten Viki
Viki is a global TV site and the ultimate destination for K-Drama and Asian entertainment. Together with Soompi, the online K-Pop authority, Viki breaks ...

Informazioni di dominio

- Anche detti **WHOIS** record;
- Contengono le informazioni un determinato dominio, tipo:
 - Date di registrazione, rinnovo e scadenza;
 - Proprietario;
 - Informazioni di contatto dell'amministratore e del proprietario;
 - Chi ha venduto il dominio;
 - DNS sui quali è presente

LIVE SESSION *pt. 1*

Mettiamo alla prova questi strumenti



Altri tools:

- Sherlock (<https://github.com/sherlock-project/sherlock>);
- Infoga (<https://github.com/m4ll0k/Infoga>);
- Archivi online (<https://archive.org/>);
- Wappalyzer (<https://bit.ly/41KWvAK>);
- Google maps (<https://www.google.com/maps/>);
- <https://osintframework.com/>.

LIVE SESSION *pt. 2*

Quante informazioni riusciamo a trovare su Mario Rossi?

[2] Richiesta di amicizia

utentestrano

Da  [utentestrano <utentestrano@proton.me>](mailto:utentestrano@proton.me)

A livesession0205@proton.me



Ciao sono Mario Rossi (detto datalyst), sono un data analyst, vuoi essere mio amico? <3