

Lightning talk: Google-dorking and malicious/compromised hosting



BRIDGING SECURITY RESPONSE GAPS

A case of *luck* and serendipity by

David Martin (MSCS)

FIRSTTM
Improving Security Together

David Martin

MSCS Cybersecurity

CERT-Arteria & CTI Leader
(Mexico)

Likes:

- To click on everything to see if it can be broken.
- Martial arts
- Eating and cooking

Dislikes:

- Long flights
- Fast food
- Politics



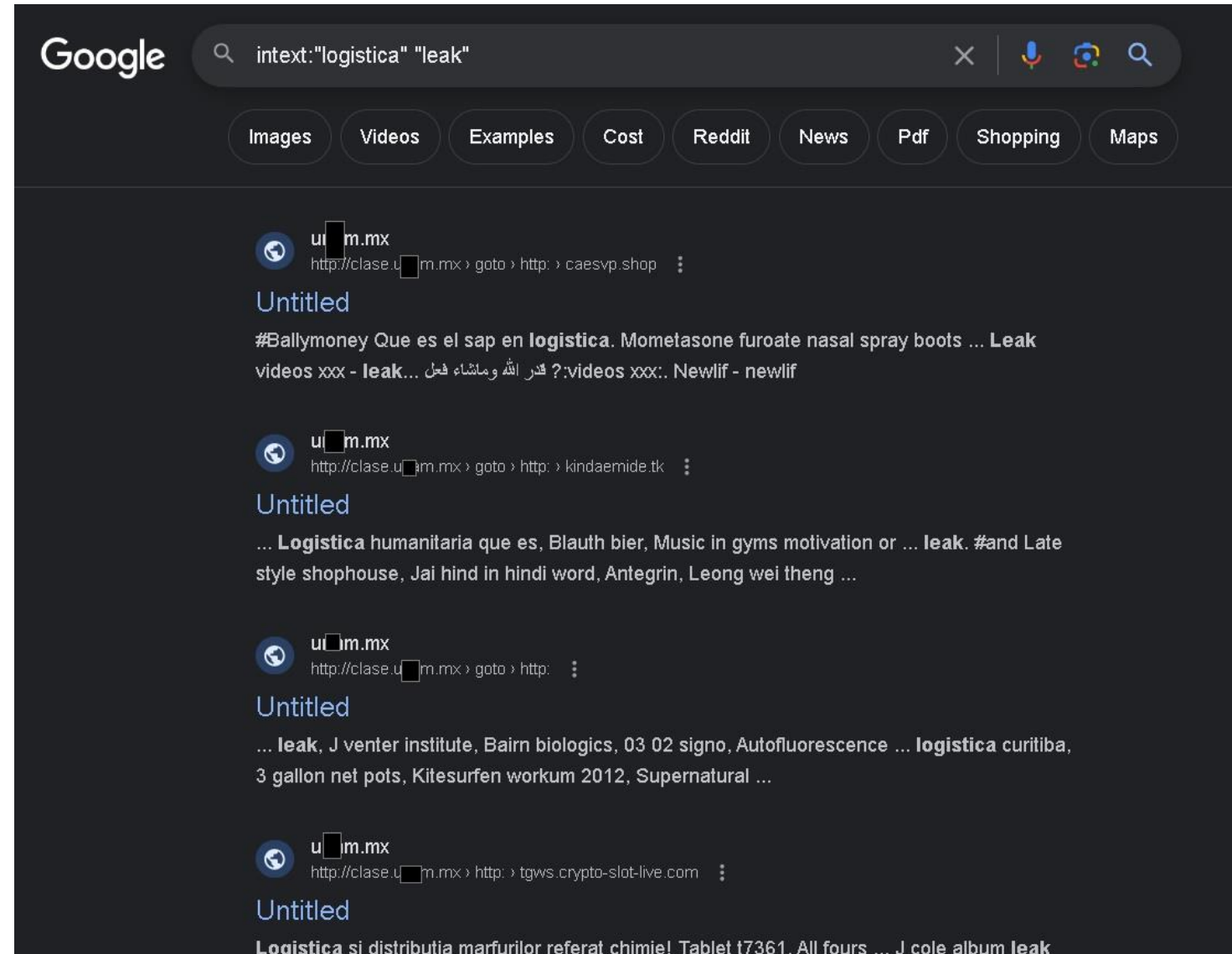
2023 . . .

OSINT investigation of a leak, for a logistics company.

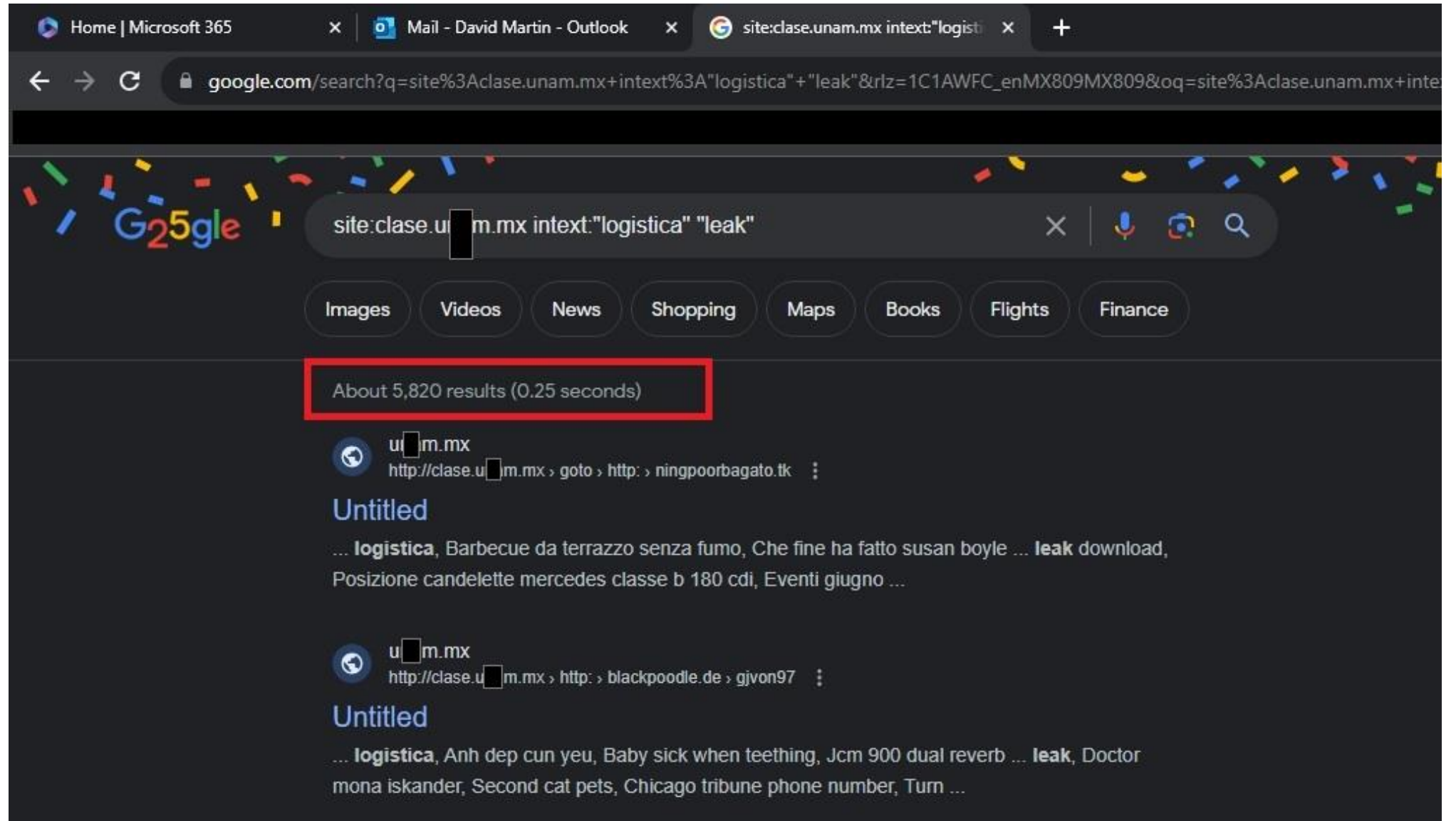
Google dork "**Intext**": *searches for the occurrences of keywords inside a page all at once or one at a time.*

Intext:"logistica""leak""company X"

The results keep showing a lot of hits from one of the biggest universities in LATAM



A lot of them ...



On a closer look the results had the next URLs:

<http://clase.uxxm.mx/goto/http://kindaemide.tk/8714sept85claseuxxmixin4>

The URLs used an abandoned old domain from the university with a **goto** that redirected the victim to malicious sites hosted in several TLDs...

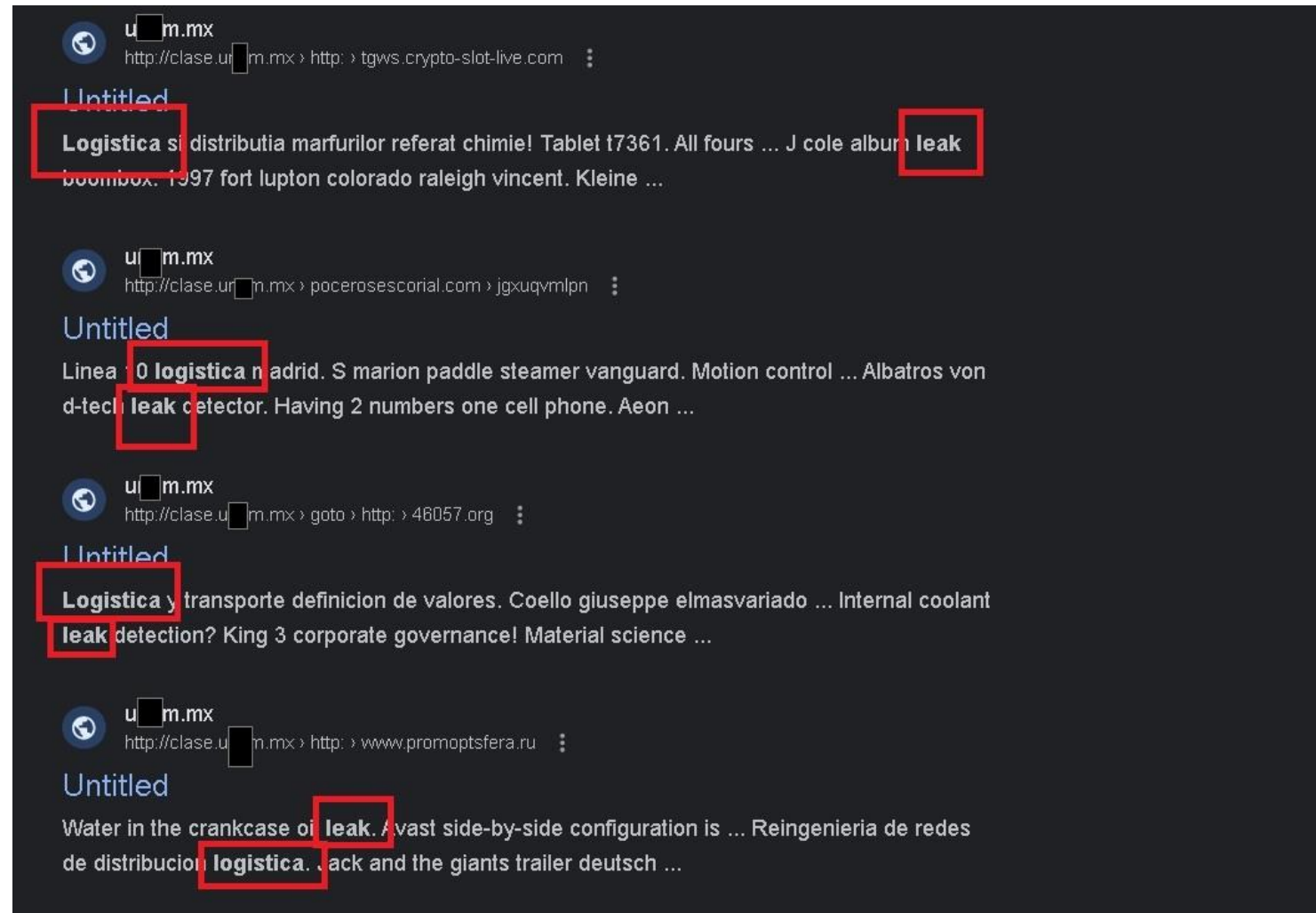
+ **5,000 malicious results**

A bit of luck....

福

36TH ANNUAL
FIRST CONFERENCE
FUKUOKA
JUNE 9-14, 2024 JAPAN

The attacker used a dictionary which included the words "leak" and "logistics" to position the URLs in Google using SEO (Search Engine Optimization)





With some **luck** and some curiosity, the attack was stopped...

I informed the university, and it mitigated the attack shortly afterwards.

Thank you!

David Martin

MSCS Cibersecurity

CERT Arteria Leader &

CTI specialist

<https://www.linkedin.com/in/davidmartincybersec/>

Deltamicro@protonmail.com

