Google-dorking and malicious/compromised hosting

A case of *luck* and serendipity by

David Martin

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

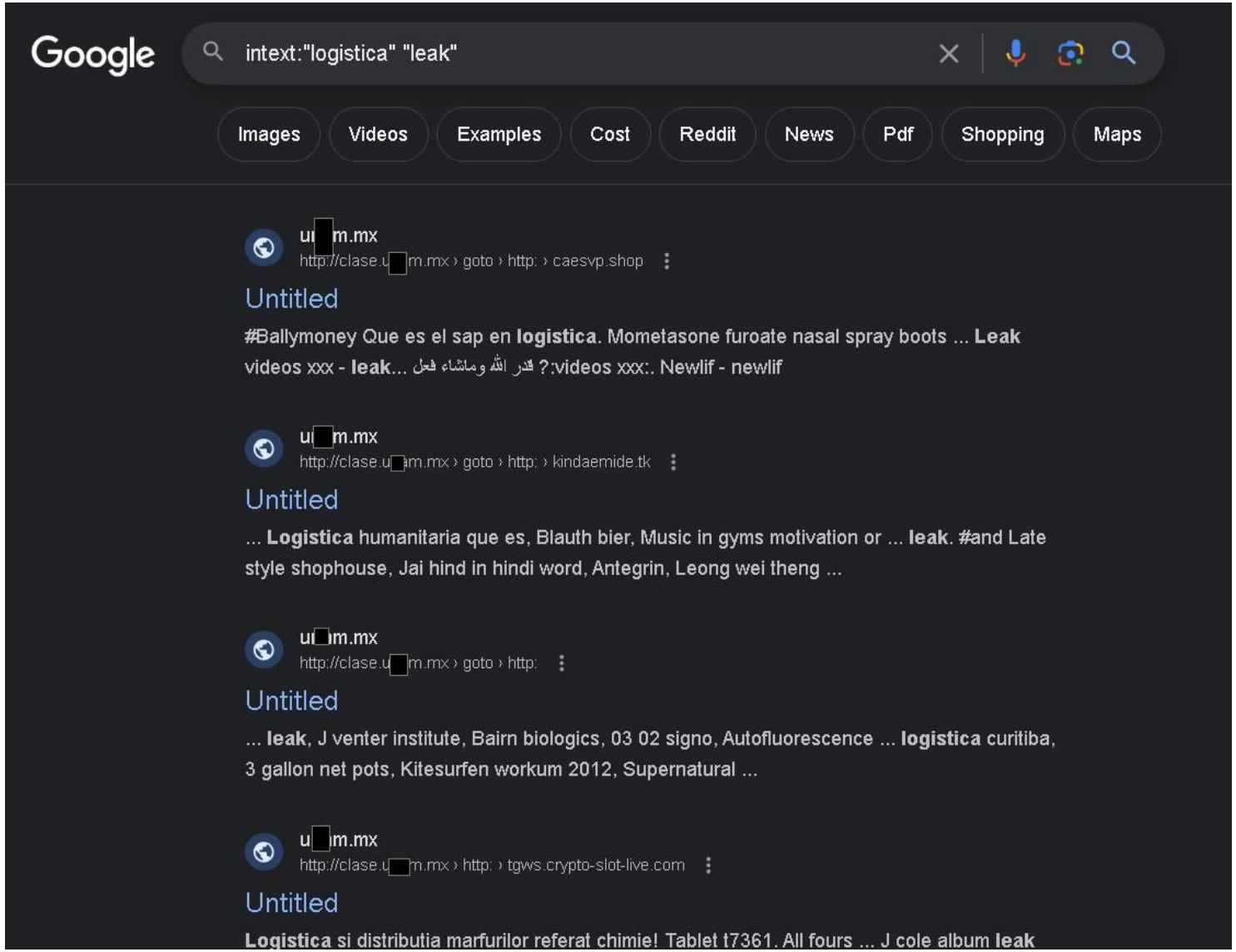
2023...

OSINT investigation of a leak, for a logistics company.

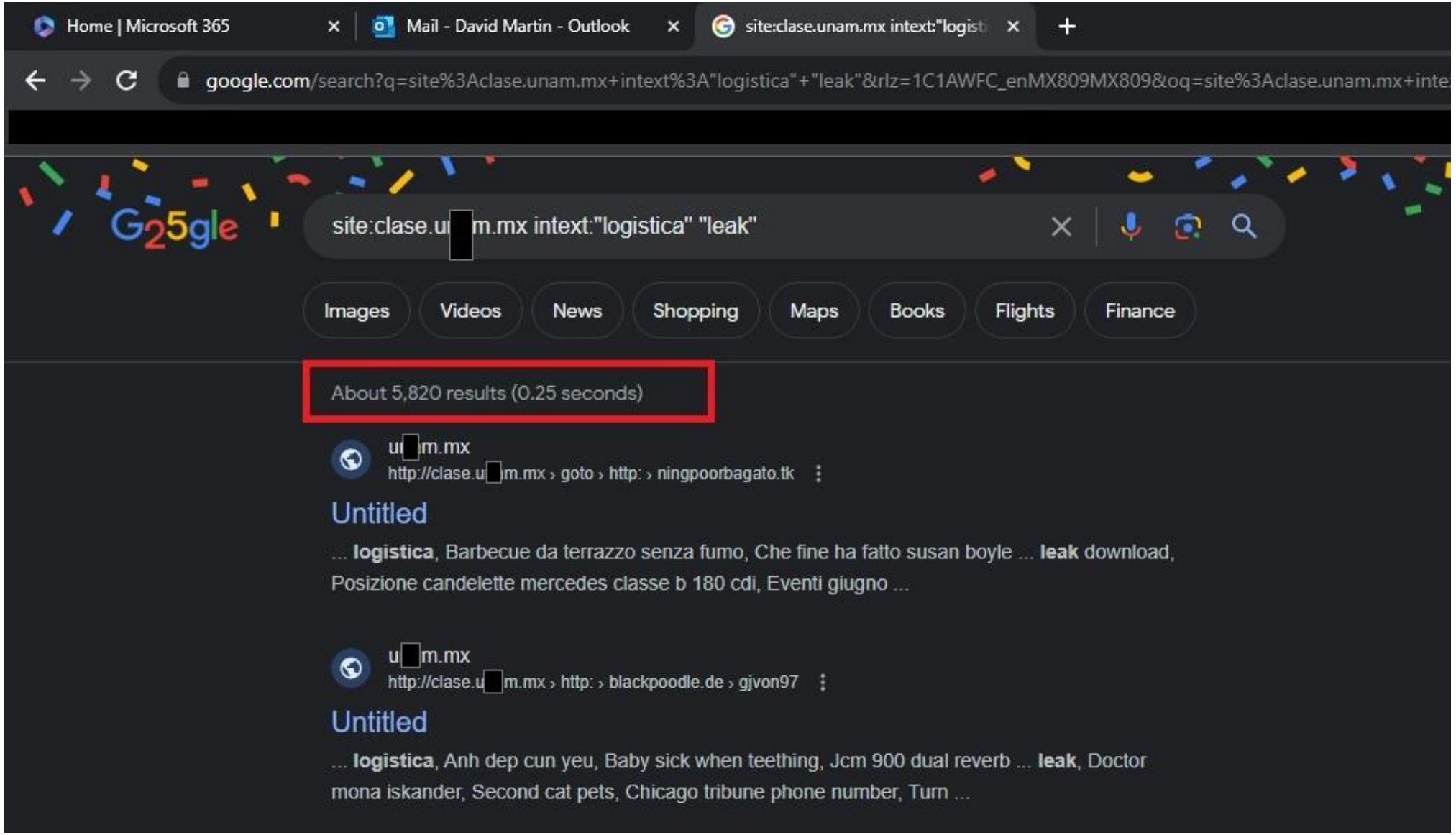
Google dork **"Intext"**: *searches for the occurrences of keywords inside a page all at once or one at a time*.

`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 ...


Home | Microsoft 365
Mail - David Martin - Outlook
site:clase.unam.mx intext:"logisti
google.com/search?q=site%3Aclase.unam.mx+intext%3A"logistica"+"leak"&rlz=1C1AWFC_enMX809MX809&oq=site%3Aclase.unam.mx+inte
G25gle
site:clase.u m.mx intext:"logistica" "leak"
Images
Videos
News
Shopping
Maps
Books
Flights
Finance
About 5,820 results (0.25 seconds)
u m.mx
http://clase.u m.mx › goto › http: › ningpoorbagato.tk
Untitled
... logistica, Barbecue da terrazzo senza fumo, Che fine ha fatto susan boyle ... leak download, Posizione candelette mercedes classe b 180 cdi, Eventi giugno ...
u m.mx
http://clase.u m.mx › http: › blackpoodle.de › gjvon97
Untitled
... logistica, Anh dep cun yeu, Baby sick when teething, Jcm 900 dual reverb ... leak, Doctor mona iskander, Second cat pets, Chicago tribune phone number, Turn ...

On a closer look the results had the next URLs:

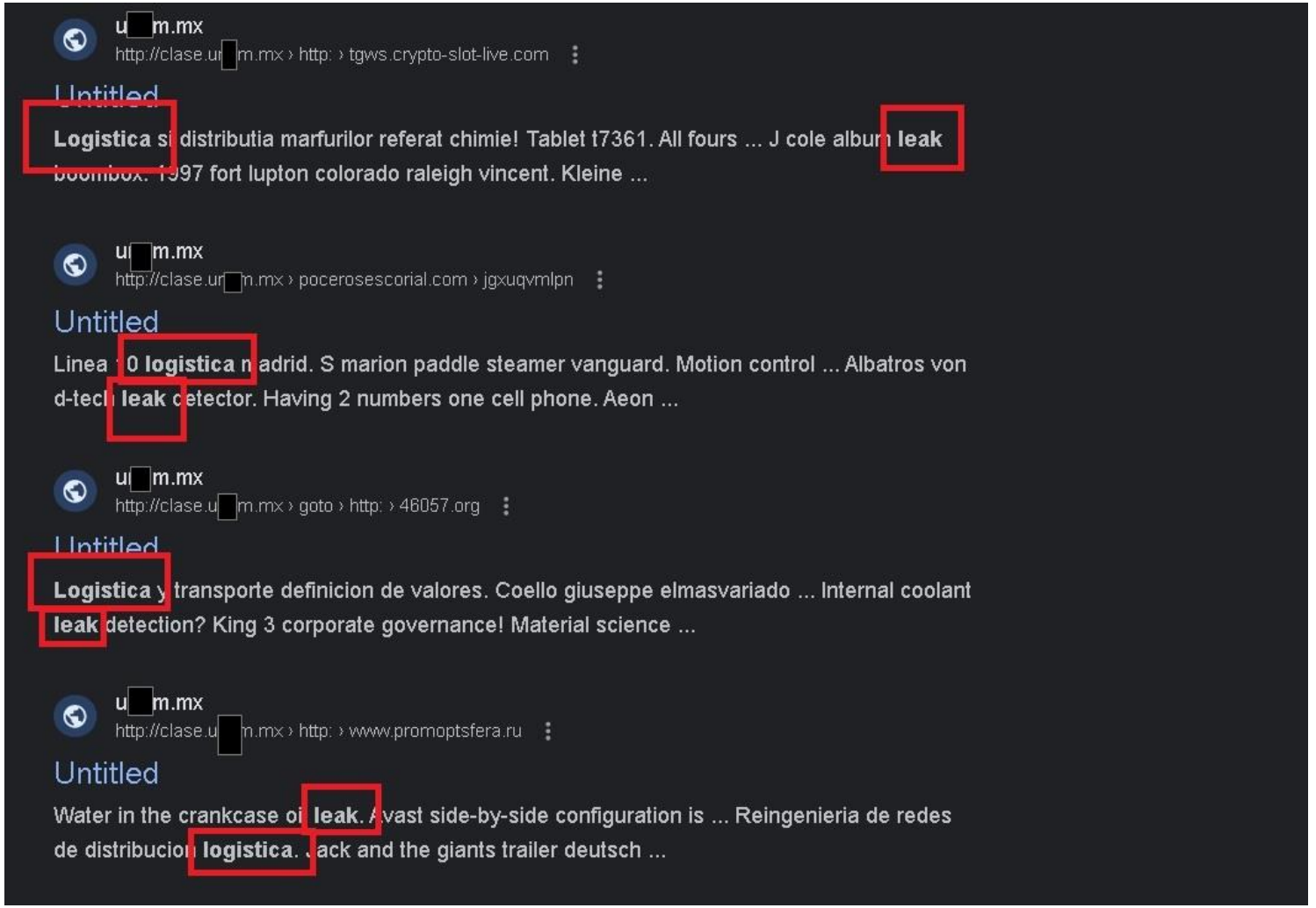
http://clase.uxxm.mx/**goto**/http:/kindaemide.tk/8714sept85claseuxxmmxin4

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....

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