TLP:GREEN

September 29, 2023

CERT-Arteria discovers extensive abuse of domain belonging to UNAM (National Autonomous University of Mexico) Library system.

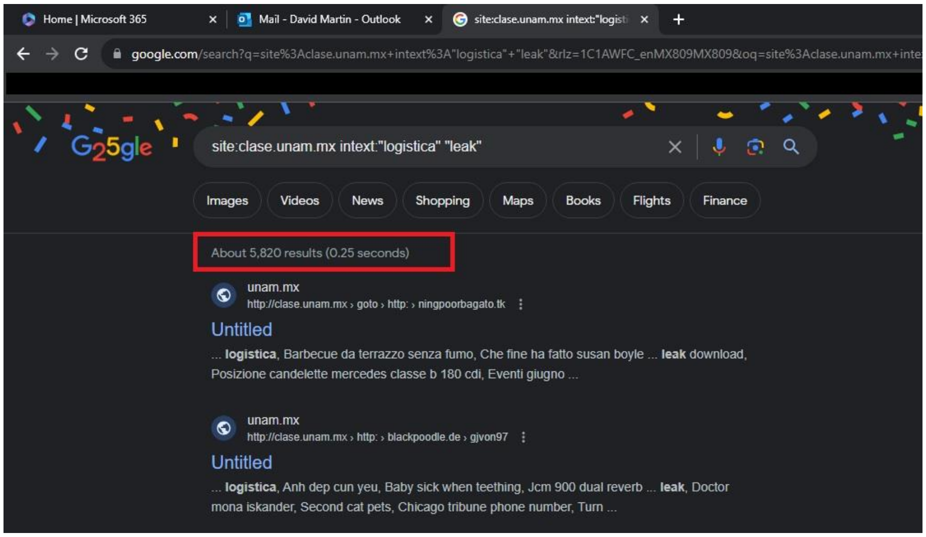
As part of cyber-patrolling and routine cyberintelligence work carried out by CERT-Arteria for various companies, MSCS David Martin discovered the extensive abuse by malicious actors of the **clase.unam.mx** domain belonging to the "General Directorate of Libraries and Digital Information Services" of the UNAM.

The clase.unam.mx domain is the previous version of the current **https://clase.dgb.unam.mx/** to which it redirects. However, it was not properly taken down and has been abused through the inclusion of a "**goto"** resource in its URLs and a large dictionary (list of keywords) to be placed in the results of search engines SEO such as Google.

In the following URL (sanitized) we can see the configuration of one of the malicious URLs which redirects to a site with malware with the domain ".ru" (Russia)

hxxp://clase[.]unam.mx**/goto/**http:/www[.]promoptssphere.**ru**/rabfosd.htm

There are currently around 6,000 malicious results with this configuration, which can be obtained using the Google Dork **site:clase.unam.mx intext:"logistica" "leak",** as can be seen in the following image.



google.com/search?q=site%3Aclase.unam.mx+intext%3A"logistica"+"leak"&rlz=1C1AWFC_enMX809MX809&oq=site%3Aclase.unam.mx+inte

[redacted]

site:clase.unam.mx intext:"logistica" "leak"

About 5,820 results (0.25 seconds)

unam.mx
http://clase.unam.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 ...

unam.mx
http://clase.unam.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 ...

This incident was reported on September 26, 2023 at 8:36 p.m. (CST) to the CERT-UNAM and university authorities (DGTIC) for mitigation. This article was published on September 29 in accordance with our disclosure policy, which states that we will publish vulnerabilities within 48 hours of the notice.

David Martin

Master in Cybersecurity
Intelligence Specialist
CERT-Arteria Leader
Ex. PBSI CERT-UNAM 13 Generation.

https://cert.arteria.com.mx/