TLP:GREEN

29 de Septiembre 2023

CERT-Arteria descubre abuso extensivo de dominio perteneciente a Bibliotecas de la UNAM.

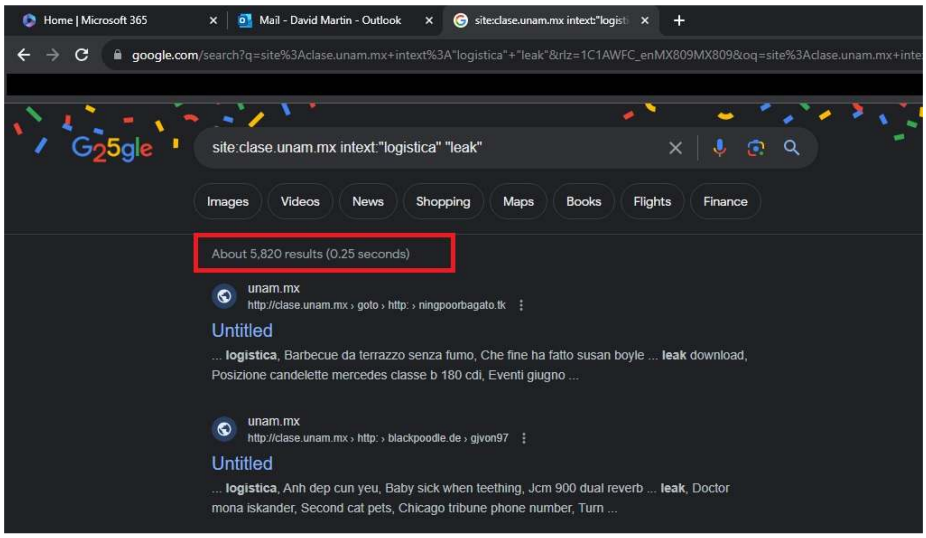
Como parte de ciberpatrullaje y las labores de ciberinteligencia rutinarias llevadas a cabo por el CERT-Arteria para diversas empresas, el Mtro. David Martin descubrió el abuso extensivo por parte de actores maliciosos del dominio **clase.unam.mx** perteneciente a la “Dirección General de Bibliotecas y Servicios Digitales de Información” de la UNAM.

El dominio **clase.unam.mx** es la versión anterior del actual **https://clase.dgb.unam.mx/** al cual redirige. Sin embargo, no fue dado de baja adecuadamente y ha sido objeto de abuso a través de la inclusión de un recurso “**goto”** en sus URLs y una lista grande de palabras clave para colocarse en los resultados de los buscadores como Google.

En la siguiente URL (sanitizada) podemos observar la configuración de una de las URLs maliciosas la cual redirige a un sitio con malware con el domino “.ru” (Rusia)

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

Actualmente se encuentran alrededor de 6,000 resultados maliciosos con esa configuración, los cuales pueden ser obtenidos utilizando el Google Dork **site:clase.unam.mx intext:"logistica" "leak"** , como puede apreciarse en la siguiente imagen.



Este incidente fue reportado el día 26 de septiembre del 2023 a las 20:36 horas (CST) al CERT-UNAM y autoridades universitarias (DGTIC) para su mitigación. El presente artículo se publicó el 29 de septiembre de acuerdo con nuestra política de disclosure, la cual indica que realizaremos la publicación de vulnerabilidades en un plazo mayor a 48 horas a partir del aviso.

David Martin

Máster En Ciberseguridad

Líder CERT-Arteria

Ex. PBSI CERT-UNAM 13 Generación.

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