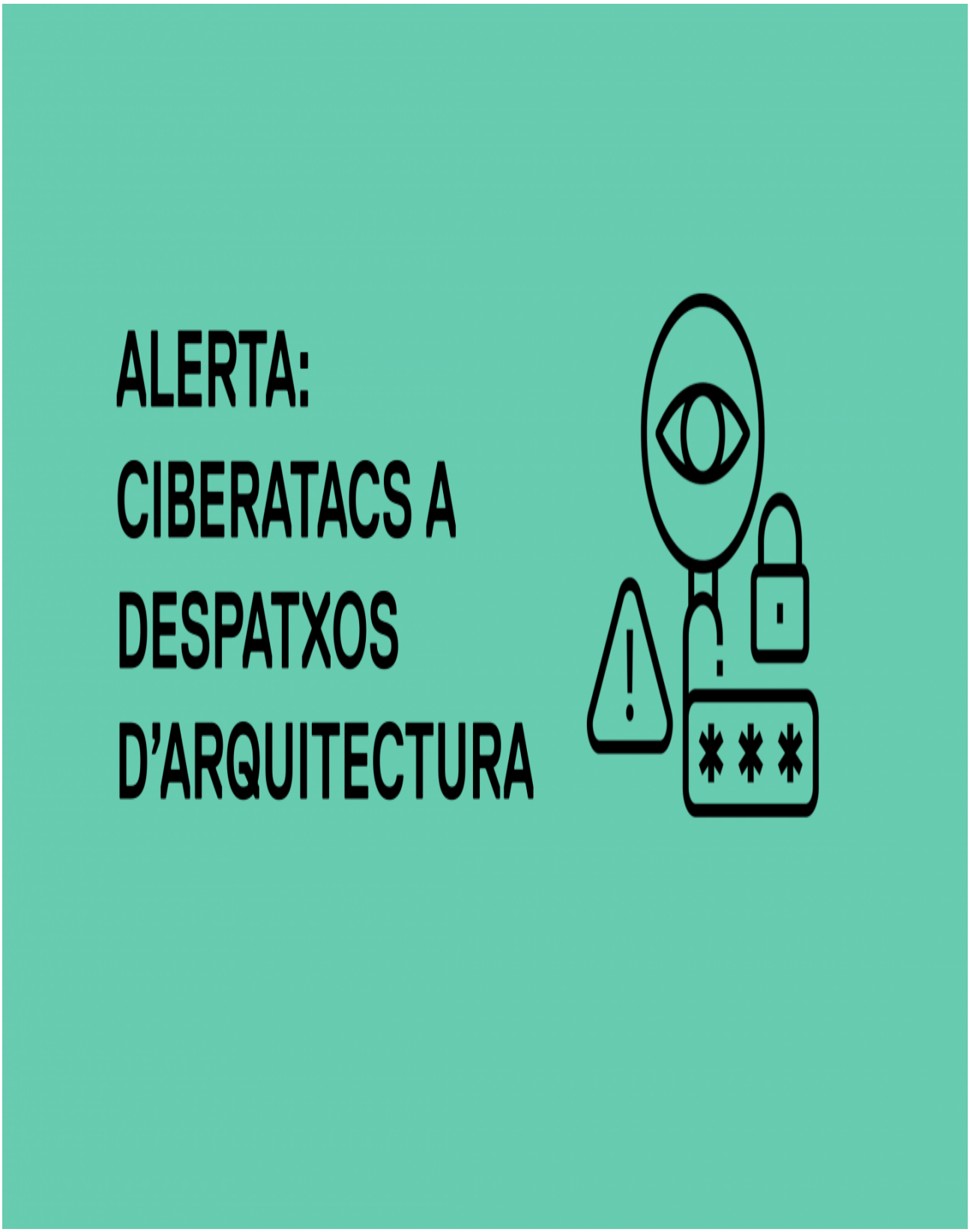
La Policia Nacional alerta de ciberatacs a estudis d'arquitectura [1]



Published:
29 August 2023

La Policia Nacional alerta que, en els darrers dies, s'han detectat diversos ciberatacs a estudis d'Arquitectura. Com a resultat de la ciberpatrulla i la col·laboració ciutadana, a

través de la secció "Col·labora" del lloc web www.policia.es [2], es té coneixement de l'auge d'una campanya de distribució del ransomware denominat **Lockbit Locker**, dirigida contra estudis d'arquitectura, mitjançant la **suplantació de l'empresa Fotoprix**, en un primer moment, i fent-se passar per propietaris de fleques o d'altres negocis.

SISTEMA DE CIBERATAC
Segons informa la Policia Nacional, en aquest cas, els atacants envien un correu electrònic a determinades empreses d'arquitectura des d'un domini del tipus "fotoprix.eu" (sense que existeixi aquest domini), o d'altres tipus (fleca, ferreteria, etc.), sol·licitant pressupost per realitzar una reforma a la seu de l'empresa.

Després de diversos correus electrònics, els atacants proposen concretar una data per a una reunió inicial i així poder fixar el pressupost, però, com a requisit previ a aquesta, envien mitjançant "WeTransfer" uns documents amb les especificacions de la reforma perquè l'empresa d'arquitectura pugui ajustar el pressupost al màxim a les necessitats.

Quan la víctima descarrega el fitxer i l'executa al seu ordinador, aquest queda automàticament xifrat i els ciberdelinqüents sol·liciten un rescat per recuperar els fitxers, les instruccions del qual queden reflectides dins d'un fitxer .txt que s'hi copia a l'equip afectat.

La campanya ha assolit un nivell de sofisticació molt alt, ja que les comunicacions dels ciberdelinqüents resulten totalment concordants i congruents, per la qual cosa les víctimes no sospiten res fins que pateixen l'encriptació dels equips.

RECOMANACIONS PER EVITAR SER VÍCTIMA DE CAMPANYES DE RANSOMWARE

- No obrir correus provinents de remitents desconeguts o dels quals no s'hagi sol·licitat informació prèvia.

- Contactar telefònicament amb el client per verificar la informació.

- No descarregar arxius adjunts de correus provinents de remitents desconeguts.

- Mantenir sempre actualitzat el sistema operatiu i l'antivirus.

- Realitzar periòdicament còpies de seguretat independents.

Per denunciar qualsevol incident, dirigir-se a **seguridad.logica@policia.es** [3]
Informació de l'Institut Nacional de Ciberseguretat enllaç [4]

Links
[1] https://arquitectes.cat/en/node/39226
[2] http://www.policia.es
[3] mailto:seguridad.logica@policia.es
[4] https://www.incibe.es/empresas/avisos/campana-de-correos-electronicos-maliciosos-que-pretenden-infectar-equipos-con