Después de 5 días Google desbloquea acceso a nuestra web hackeada para minado de criptomonedas

Ya puede visitar nuestra web con absoluta tranquilidad.

El ataque informático había introducido código malicioso en un archivo central de la plantilla que ejecuta nuestra web.

Nuestros visitantes sólo han sido usados para el minado de una criptomoneda.

El ataque no introducía código en su ordenador.

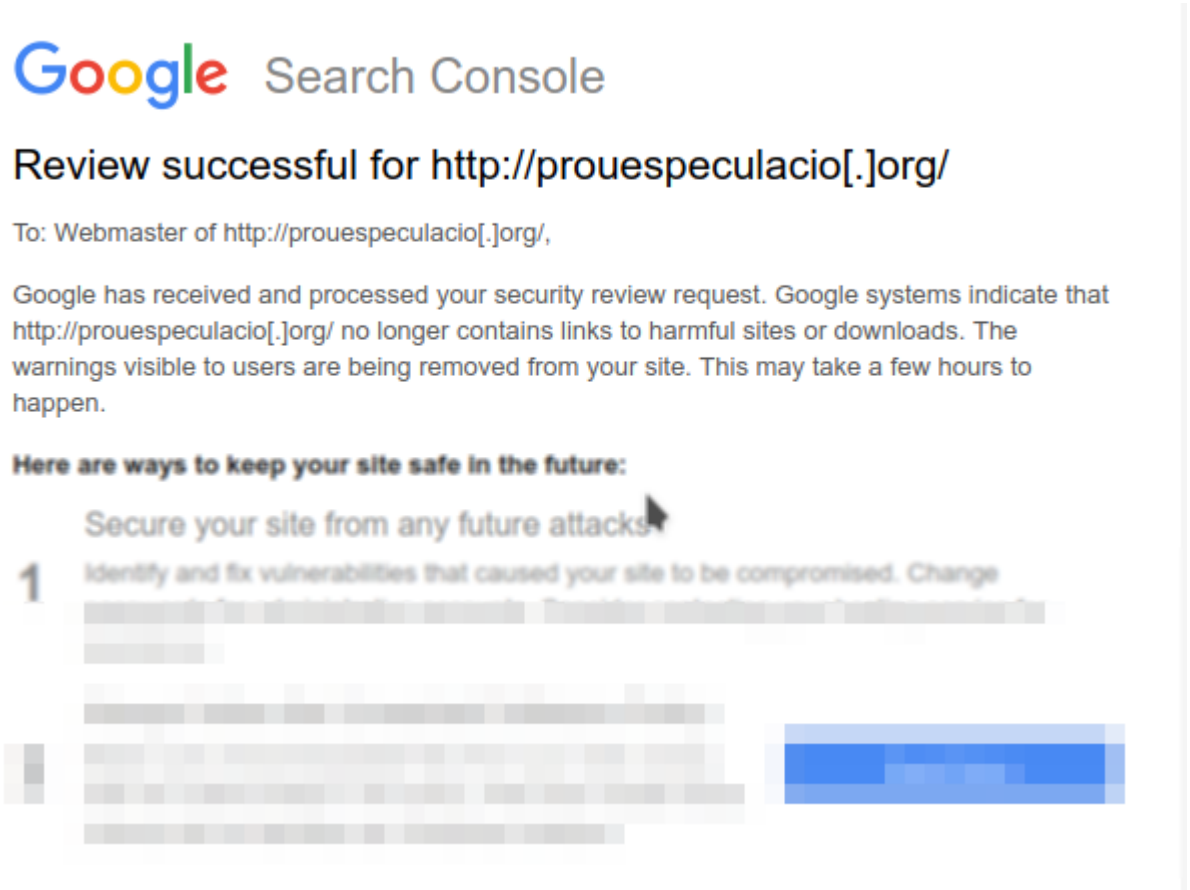
Google ha desbloquedo nuestro dominio después de que nuestros técnicos han eliminado el fragmento de malware detectado en la plantilla principal del wordpress de nuestro subdominio: http://500×20.prouespeculacio.org. De resultas del bloqueo a nuestro dominio las visitas bajaron de las mil diarias a poco más de 100.

El código malicioso apunta a la página [https://cdns.ws/lib/googleanalytics.js] alojada en el dominio

considerado peligroso [https://cdns.ws]. Al visitar la página principal de este dominio, sólo hay una pantalla en blanco. Creemos que el script fue introducido por la técnica de "fuerza bruta" en un archivo central (functions.php) de la plantilla que ejecuta nuestra web.

El script se encontraba en nuestro dominio. No introducía código en su ordenador sino que esclavizaba su cpu y tarjeta gráfica para procesar datos de alguna cadena de bloques (blockchain) de criptomonedas, actividad que requiere mucha energía para procesar datos. Nuestra sospechas se iniciaron a finales de noviembre cuando descubrimos una anomalía en la web: en cuanto te conectabas a ella automáticamente la cpu se ponía a usar el 100% de los recursos y su temperatura subía a casi 70º C. Sucedía con cualquier navegador y cualquier sistema operativo que usamos(distribuciones de Linux y Windows7). Ese comportamiento nos llevó a contactar con los servicios de nuestro hosting que finalmente detectaron la intrusión. No es nuevo bajo el sol. Dos webs como Movistar (1) y Bolsamania (2) también han tenido esos problemas con la explosión de las criptomonedas. Seguramente 2018 habrá una explosión de código malicioso en ese sentido. Si usted cree que su cpu sobreactúa al conectarse a una página web puede existir ese problema con el dominio que visita. Si por la causa que fuere debe entrar igualmente nosotros hemos comprobado que al cerrar el navegador que usa, varias veces, el script deja de funcionar seguramente porqué la conexión se vuelve inestable y el script descarta esa cpu.

Nuestro hosting y Google han certificado ya el correcto funcionamiento de nuestro subdominio:



Pues nada, gracias por visitarnos nuevamente!!!

.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-

Más información:

- (1) elconfidencial, Auto-boicot de Movistar: inyecta un virus en su web para protegerse de los ‘hackers.
- (2) adslzone, Un blog de Bolsamanía ha sido hackeado para minar criptomonedas.
- eldiario.es, Que no te minen la moral: cómo evitar que usen tu ordenador para ganar dinero sin que lo sepas.