¿QUÉ ES EL PHARMING?

Consiste en redirigir las solicitudes de un usuario a sitios web fraudulentos que son prácticamente iguales que el sitio web legítimo. Los atacantes manejan gran cantidad de equipos informáticos donde alojan los sitios clonados o fraudulentos, en los que pueden capturar información confidencial de la víctima (nombre de usuario, contraseñas, datos bancarios, etc.) o pueden instalar malware en su equipo informático.

¿Qué tipos de pharming existen?

- **Pharming local:** consigue introducir un virus o un troyano en el equipo de la víctima; es decir, es pharming mediante malware instalado al descargar archivos adjuntos de algún email fraudulento o de un sitio web de poca confianza y se encarga de alterar los registros de nombres en el archivo "hosts" cambiando las direcciones de IP almacenadas, de manera que el computador envía los datos al sitio falsificado. Este tipo de ataque solo afecta un computador.
- **Envenenamiento del caché DNS:** Este método se centra en dañar el propio servidor DNS, de manera que el hacker reescribe las reglas que marcan el envió de datos hasta un dominio específico para redirigirlo a una dirección IP del sitio web falsificado. En este caso, el ataque se dirige contra un servidor y no contra un único computador, con potencial de afectar a muchos usuarios a la vez.
- **Drive-By pharming:** Esta técnica ataca directamente los firewalls o routers y cambia la dirección del servidor DNS a la de un servidor controlado por el atacante, quien resolverá las direcciones como desee. Es una técnica de uso más reciente debido al uso de plataformas Wi-Fi, que en muchos casos utilizan enrutadores con claves administrativas que los usuarios no han cambiado.

¿Cómo saber si hemos sido víctimas de pharming:

1. Cuando se hayan producido pagos desconocidos en nuestra tarjeta de crédito o débito.
2. Cuando se nos pida confirmar un cambio de contraseña que no ha solicitado.
3. Publicaciones en redes sociales o aplicaciones de mensajería que no hemos enviado.
4. Aparición de nuevas aplicaciones en nuestros dispositivos o equipos que nosotros no hemos descargado.

Telf: 2236-092 / Conmutador 3955-900
dntic.direccion@policiaecuador.gob.ec
Dirección Nacional de Tecnologías de la Información y Comunicación
Departamento de Seguridad de las TIC´s

¿Cómo protegerse contra el pharming?

- Al visitar un sitio web debemos asegurarnos de que la URL está bien escrita; es habitual que la URL de un sitio falso tenga alguna letra cambiada (por ejemplo, “ez.com” en vez “es.com”). Y a su vez que la URL empieza por HTTPS; esa “S” significa seguro y que la web se cifra.
- Evitar sitios web sospechosos o de poca confianza es clave para evitar ataques de pharming, sobre todo si vas a descargar archivos de ellos.
- No dar click en vínculos y archivos de origen desconocido, para evitar instalar malware en nuestro computador.
- No ignorar al antivirus es importante, tanto como tener uno instalado. Un buen antivirus, que se actualice con regularidad, nos avisará cuando entramos en sitios web sospechosos o infectados.
- Hay que tener mucho cuidado con las ofertas demasiado buenas para ser verdad; no es poco habitual que los atacantes creen ofertas atractivas fraudulentas para atraer víctimas.