https://info.nodo50.org/Ola-de-spam-con-origen-en-cuentas-robadas.html

Ola de spam con origen en cuentas robadas

- Nodo50 - Noticias Técnicas -

Fecha de publicación en línea: MiÃ©rcoles 16 de junio de 2021

El martes 15 de junio comenzó un envío masivo de mensajes con enlaces sobre criptomonedas y pornografía. Probablemente se han enviado decenas de millones de mensajes, de los que unos cuantos miles iban dirigidos a direcciones de correo alojadas en Nodo50. La mayoría los hemos detenido con filtros basados en el contenido.

Una característica destacable de esta ola de spam es que el remitente de los mensajes no ha sido falsificado, sino que han usado relamente esas cuentas mediante contraseñas robadas.

Por eso los mensajes que llegaban a nuestros servidores provenían de los servidores legítimos de servicios de correo como Gmail, Yahoo y Hotmail. Y eso hacía mas complicado filtrarlos.

En este artículo de del blog del antivirus Eset podéis ver mas detalles de esta ola de spam.

Los mensajes contenían enlaces del servicio acortador de URLs bit.ly, y también del servicio feedproxy de Google. Nos hemos visto obligados a bloquear todos los mensajes que contengan ambos tipos de direcciones web, lo que implica que también habremos bloqueado mensajes legítimos, e incluso mensajes vuestros reenviándonos ejemplos de este spam. Lo hemos hecho de forma que a la persona que envía se le informe claramente de la causa del bloqueo, para que pueda volver a enviar el mensaje sin ese enlace.

Una pregunta habitual es ¿cómo saben los atacantes cual es la contraseña de esos buzones?

Lo mas probable es que la hayan obtenido de las, cada vez mas frecuentes, filtraciones de datos que se publican en Internet. Son filtraciones de datos de usuarios/as o clientes de servicios concretos. Pero el problema es que muchas veces la gente reutiliza contraseñas, entre ellas la de sus buzones de correo.

Por tanto los atacantes solo tienen que ponerse a probar en múltiples sitios con esas mismas credenciales. Ponemos un ejemplo no real para que se entienda mejor:

- En mayo de 2016 se filtraron 164 millones de nombres de usuarios/as y contraseñas de Linkedin (esto es real, esa filtración existió). El nombre de usuario/a era una dirección de correo electrónico.
- Los atacantes ven que había un usuario de Linkedin con login pepesapo@gmail.com y contraseña 6$fde_Y.)ysrh3d=udr5Yx;ue4"d
- Lo que harán será probar si esa contraseña sirve para entrar en la cuenta pepesapo@gmail.com
- Y también probar a entrar con ese mismo email y contraseña en multitud de servicios: Facebook, Twitter, etc.

Y todo esto sin que sea un ataque dirigido, sin que tengan información especial sobre pepesapo. Lo hacen de forma automatizada con miles o millones de cuentas. Y sin que importe lo segura que sea la contraseña.

Si además tienen algún interés especial en pepesapo, y conocen mas datos, podrían hacer un ataque mas dirigido. Por ejemplo si conocen su NIF intentar entrar en webs de bancos con el NIF y esa contraseña.

Por esto es tan importante no reutilizar contraseñas, en particular las de las cuentas de correo, que son la llave para entrar a otros servicios (para resetear contraseñas, por ejemplo). Y cambiarlas cada cierto tiempo.

En esta web www.haveibeenpwned.com podéis comprobar si vuestra direcciones de correo ha estado incluida en alguna filtración de datos. Si es así lo mejor es que cambiéis la contraseña.

Actualización 17/junio/2021: El jueves 17 de junio, por la mañana, hemos retirado el bloqueo a mensajes que contengan enlaces de bit.ly ya que hemos observado que el tráfico de mensajes de esta ola de spam practicamente ha desaparecido, así evitamos bloquear mensajes con un uso legítimo de bit.ly

Actualización 23/junio/2021: Reactivamos el bloqueo a mensajes que contengan enlaces de bit.ly, ya que vuelven a las andadas. Seguramente hayan conseguido otro montón de cuentas robadas para hacer los envíos.

Actualización 25/junio/2021: Volvemos a retirar el bloqueo por la mañana pues ha cesado la segunda ola de spam. Bit.ly ha desactivado muchos enlaces maliciosos y seguramente los grandes proveedores de correo han bloqueado las cuentas robadas que se usaban para hacer los envíos.