Escrito por VM
Xoves, 11 Setembro 2014 21:31

A Policía Nacional, a través da súa conta de Twitter recomenda aos usuarios de contas de Gmail que verifiquen se o seu enderezo puido ser filtrado no último ataque rexistrado nos servidores de Gmail, que comprometeron a seguridade das contas de correo de máis de 5000 usuarios.

Realmente a vulnerabilidade non foi do propio sistema, si non a través dunha táctica de "malware" ou "phising" moi utilizada tamén para captar datos bancarios. O sistema consiste no envío de correos electrónico suplantando a identidade doutra persoa para solicitar os datos de acceso. A vítima crendo que se trata dunha mensaxe oficial, acceder a unha web trampa que capta os datos de acceso sin que o usuario se percate que están accedendo a unha web fraudulenta.

Isto máis ou menos sería o que aconteceu no caso do "phising", pero no caso do "malware" a infección sería a través do propio ordenador da vítima algo que propagaría a vulnerabilidade xa que todos os usuarios que accedesen a súa conta de Gmail dende ese ordenador quedarían expostos de igual xeito até que se elimine e desinfecte o equipo.

Google ainda non se pronunciou a respecto, e a nova quedou tapada en parte polo lanzamento do novo teléfono de Apple onte memso. Os medios especializados comentan que realmente trátase de información "antiga" é dicir, listas de usuarios con correos antigos que non representan un volumen real de usuario, non obstante, comentan que ao redor do 60% dos

correos e contrasinais son lexítimos, unha crifra alarmante da que non hai resposta aínda por parte do xigante americano.

Usuarios comentaron nos foros que están a recibir ataques de "Spam" e "phising" nas súas contas de Gmail, como consecuencia da filtración.

A Policía recomendou hoxe unha ferramenta web para verificar se a nosa conta de correo quedou exposta a esta vulnerabilidade, pese a todo, Google advertiu aos seus usuarios que non poñan o seu enderezo en calquera ferramenta que se atopen na rede para verificar se foron comprometidas. Aínda así, a web publicada pola Policía parece a máis segura neste momento.

Si tienes GMail, igual te han robado la contraseña. Mira si te ha afectado el ataque https://t.co/6qo1UPl3Bv
¡En cualquier caso, CÁMBIALA!

— Policía Nacional (@policia) septiembre 11, 2014

Qué facer en caso de que o noso correo quedara exposto?

Primeiramente tranquilidade. O primeiro que deben facer os usuarios é instalar un antivirus no seu equipo. E se teño un Mac? tamén, o malware e os troyanos non afectan só a equipos Windows. Existen ferramentas gratuítas de instalación e verificación como a de Avast, que poden ser eliminadas unha vez analizado o equipo.

Unha vez asegurado o equipo, é necesario cambiar o contrasinal da conta de correo por unha nova. O novo contrasinal ten que ser forte, algo que debería aplicar tamén ao resto dos seus contrasinais nas redes sociais ou ferramentas web. O 1234 xa pode aparcalo e olvidalo, así como o seu ano de nacemento, o seu número de DNI ou o seu número de teléfono. Eses non son contrasinais seguros.

Busque un contrasinal que non leve no medio o seu nome de usuario, é dicir, se a súa conta de correo é pericodelospalotes@gmail.com o que non pode é ter un contrasinal que sexa "pericodelospalotes" porque son dos primeiros en quedar expostos ante un ataque.

Fonte . - Lifehacker