



Aproximadamente dos millones de contraseñas de sitios como Yahoo!, Facebook e incluso Google fueron publicadas en varios foros de Internet, de acuerdo con una nota de BBC News.

En la publicación indican que esta acción pudo ser por un grupo criminal que consiguió los accesos introduciendo códigos maliciosos que registra las pulsaciones de teclas cuando eran escritas en los equipos de los propios usuarios.

El investigador de seguridad Graham Cluley dijo que aún no se sabe el alcance que puede tener porque se sabe «que el 30 o 40% de las personas utilizan la misma contraseña en diferentes websites».

El sitio que contiene las contraseñas fue descubierto por los investigadores que trabajan para la empresa de seguridad Trustwave.

En una entrada de su blog esbozando sus hallazgos, el equipo dijo que creía que las contraseñas se habían cosechado por una gran botnet – conocido como Pony – que había recogió información de miles de ordenadores infectados en todo el mundo.

Una botnet es una red de máquinas controladas por delincuentes gracias a un software malicioso que había sido instalado en los ordenadores sin el conocimiento del propietario.

El servidor contenía los datos de acceso a Facebook de 318 mil personas, información para ingresar a 70 mil cuentas de Gmail, Google y YouTube, 60 mil a Yahoo!, 22 mil a Twitter y ocho mil de LinkedIn, entre otras.

Trustwave dijo que había notificado a los sitios y servicios afectados antes de publicar la entrada de blog, pero su análisis de las contraseñas mostró que la más popular, que se encuentra más de 15 mil veces en la base de datos, era «123456».

LA VERSIÓN DE FACEBOOK

Hace unos momentos, los voceros de Facebook omitieron su declaración respecto al caso:



Roban y publican 2 millones de contraseñas de Facebook y Twitter

«Aunque los detalles de este caso aún no están claros, parece que las computadoras de las personas afectadas fueron atacadas por hackers utilizando malware para robar claves directamente desde sus navegadores».

«Como medida de precaución, hemos iniciado un restablecimiento de contraseña para las personas cuyas contraseñas se han visto afectadas. Las personas pueden protegerse a sí mismas utilizando Aprobaciones de Login y Notificaciones, en su configuración de seguridad».

«Así, recibirán una notificación cuando alguien trata de acceder a su cuenta desde un navegador no reconocido y nuevos inicios de sesión requerirán un código de acceso único generado en su teléfono móvil.»

Fuente: vanguardia