https://info.nodo50.org/Cuida-tu-sistema-y-tus.html

Alerta sobre programas de FTP modificados

Cuida tu sistema y tus comunicaciones: ¿De dónde te bajas los programas que usas?

- Nodo50 - Noticias Técnicas -

Fecha de publicación en línea: MiÃ©rcoles 5 de febrero de 2014

Hola, hemos detectado y detenido algunos ataques que aprovechaban vulnerabilidades explotadas desde escenarios que responden al mismo patrón: quien pone los *scripts* sabe la contraseña de la conexión FTP, y en unas horas la web es usada como *malware* contra terceros.

En unos de nuestros manuales Si tienes problemas con el FTP recomendamos Filezilla (a modo de ejemplo porqué hay muchos más) como cliente FTP para hacer las conexiones de mantenimiento de la web.

Recientemente se ha detectado que circulan versiones fraudulentas de este programa que podrían poner en riesgo la confidencialidad en la gestión de las contraseñas, habilitando un agujero de seguridad para insertar *scripts* y codigo malicioso en nuestras webs, y luego lanzar desde ahí ataques de *spam* o *phishing*.

Si usamos Filezilla es recomendable revisar si tenemos alguna de las versiones fraudulentas. En el menú **Ayuda** > **Acerca de** puedes obtener una ventana como la de la imagen para saber si tienes una de las versiones afectadas. [https://info.nodo50.org/local/cache-vignettes/L400xH203/about_windows-6b03f.jpg]

Ante la duda, es recomendable desinstalar el programa y descargar una nueva versión. **La descarga es importante. Hay que descargarlo siempre desde la web oficial del programa o un sitio de confianza absoluta**, en el caso de Filezilla, https://filezilla-project.org/

Actualmente en Nodo50 hay más de 1100 organizaciones que tienen al menos una web alojada. Esto implica que se conecten a nuestros servidores un elevado número de personas. No todas las personas que se conectan lo hacen del mismo modo, ni con los mismos conocimientos técnicos. Entre esta variedad encontramos situaciones que os vamos reportando cuando potencialmente pueden afectar a los demás proyectos y por eso os pedimos que difundáis esta nota entre la gente que ha usado las claves de acceso FTP de la web. De nuevo, ante la duda, es recomendable empezar de cero y cambiar la contreseña.

Como siempre, ante cualquier contingencia puedes escribir a ayuda@nodo50.org o llamarnos al 915488348

Mas información:

- FileZilla Has an Evil Twin that Steals FTP Logins
- Advisory: Malware downloads on third-party websites
- Malformed FileZilla FTP client with login stealer