Detectan la presencia de un rootkit en servidores web Linux

Los investigadores de Kaspersky Labs han informado de la presencia de una nueva forma de **malware que se aprovecha de la actividad de equipos Linux que actúan como servidores web: Rootkit.Linux.Snakso.a**.

Éste **permite a atacantes potenciales inyectar código HTML malicioso** en cualquier web alojada a la que acceden los navegadores en dichos servidores, incluyendo supuestas páginas de error y expandiendo sus zarpas por decenas o cientos de sitios al mismo tiempo.

¿Cómo? Sustituyendo el código que generan los paquetes TCP/IP con otro nuevo. A continuación, el malware se conecta a una red de comando y control con una contraseña cifrada.

La peligrosidad se encuentra, precisamente, en que este malware es catalogado como rootkit, lo que quiere decir que permite un acceso de privilegio continuo a los equipos afectados siendo capaz, al mismo tiempo, de mantener su **presencia oculta a ojos de los adiministradores**.

“Parece ser el siguiente paso en las operaciones cibernéticas de inyección iFrame”, dice el miembro de Crowdstrike, Georg Wicherski, tal y como recoge Ars Technica. “También podría ser utilizado en un ataque Waterhole para llevar a cabo un ataque dirigido contra un público objetivo específico sin dejar mucho rastro forense”.

Según lo descubierto, Rootkit.Linux.Snakso.a.ha sido diseñado para servidores que corren la **versión de 64-bit de Debian Squeeze y NGINX**.