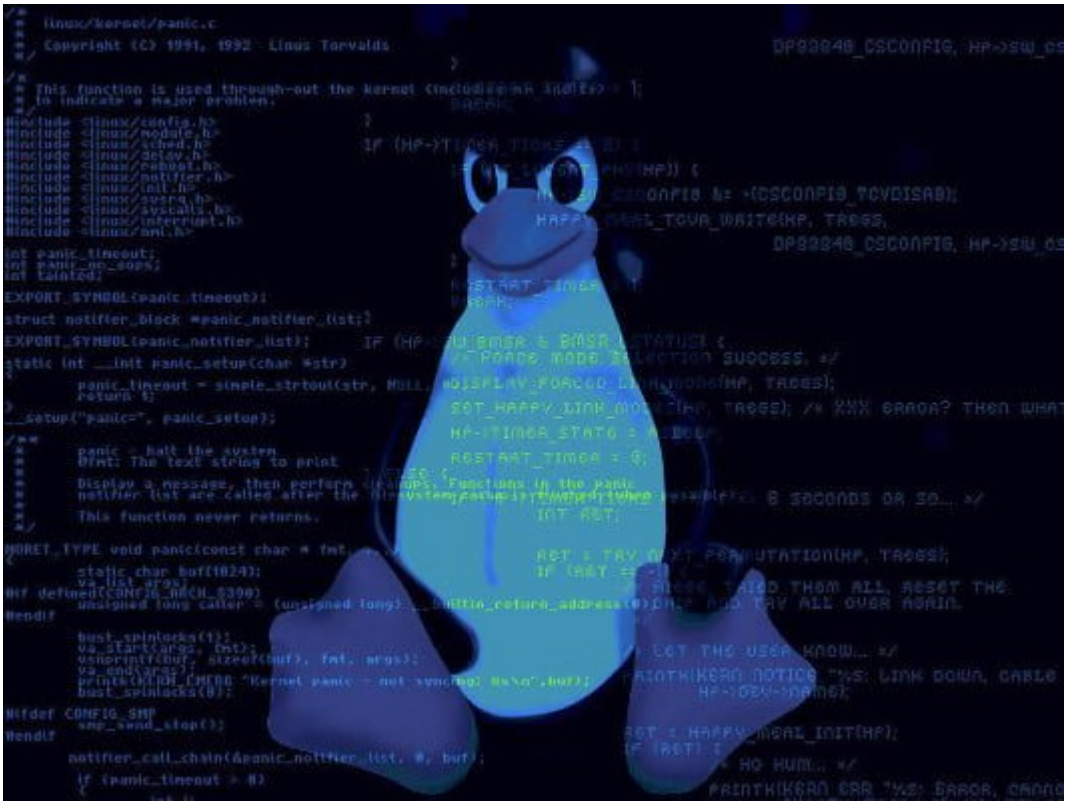
10.000 Servidores Linux Infectados Para Redirigir Medio Millón De Visitantes A Malware Cada Día

La empresa de seguridad ESET ha publicado hoy un análisis técnico en Linux/Ebury. Se trata de un backdoor en Open SSH el cual ha robado credenciales. Durante las últimas semanas , miles de víctimas han sido notificados de que sus servidores han sido infectados, con los detalles de la publicación de hoy se pretende aumentar la sensibilización de los usuarios. Esta infeccion masiva ha sido apodada como: «**Operación Windigo**«, el esquema se ejecuta en una infraestructura totalmente alojado en computadoras comprometidas: 25.000 servidores Linux en total durante los dos últimos años, con más de 10.000 infectados actualmente.

El número es significativo, ya que **ESET** señala, cada uno de estos sistemas tiene acceso a ancho de banda considerable, almacenamiento, potencia de cómputo y memoria. El grupo detrás del **malware** utiliza los sistemas infectados para robar credenciales , re dirigir el tráfico de Internet a contenido malicioso, y enviar **mensajes de spam**. El **malware** ha tenido un impacto particularmente grande en **Alemania , Francia, el Reino Unido y los EE.UU**.



Los **servidores infectados** se utilizan para re direccionar la mitad de un millón de visitantes de la web a contenido malicioso diariamente, de acuerdo con la estimación de la empresa de seguridad. Además, **ESET** cree que los atacantes son capaces de enviar más de **35 millones de mensajes de spam al día** con la infraestructura actual. Los sistemas operativos afectados por el backdoor incluyen **Linux, FreeBSD, OpenBSD, OS X, y Windows (con Perl corriendo bajo Cygwin).**