

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 infección 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.**

```
linux/kernel/panic.c
Copyright (C) 1991, 1992 - Linus Torvalds
DP98848_CSCONFIG, HP->SW_03

/*
 * This function is used through-out the kernel (including the init)
 * to indicate a major problem.
 */
#include <linux/config.h>
#include <linux/module.h>
#include <linux/sched.h>
#include <linux/delay.h>
#include <linux/cblist.h>
#include <linux/notifier.h>
#include <linux/init.h>
#include <linux/string.h>
#include <linux/sync.h>
#include <linux/irq.h>
#include <linux/interrupt.h>
#include <linux/ansi.h>
DP98848_CSCONFIG, HP->SW_03

int panic_timeout;
int panic_no_sigs;
int latched;
EXPORT_SYMBOL(panic_timeout);
struct notifier_block *panic_notifier_list;
EXPORT_SYMBOL(panic_notifier_list);
static int __init panic_setup(char *str)
{
    panic_timeout = simple_strtoul(str, NULL, 10);
    __setup("panic=", panic_setup);
}
/*
 * panic - halt the system
 * Print: The text string to print
 * Display a message, then perform cleanup. Functions in the panic
 * notifier list are called after the system has been halted.
 * This function never returns.
 */
EXPORT_TYPE void panic(const char *fmt, ...)
{
    static char buf[1024];
    va_list args;
    if defined(CONFIG_ARCH_S390)
        unsigned long caller = (unsigned long) __builtin_return_address(0);
    printk(KERN_EMERG "Kernel panic - not syncing: %s\n", buf);
    buf[0] = '\0';
}
#ifdef CONFIG_SMP
smp_send_stop();
#endif
notifier_call_chain(&panic_notifier_list, 0, buf);
if (panic_timeout > 0)
```

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).