

## Nueva Versión de Mydoom

29 de Enero de 2004

Kaspersky Labs, líder en desarrollo de software antivirus ha detectado una nueva versión de Mydoom (Novarg) - Mydoom.b.

Kaspersky Labs ha recibido reportes de infecciones por este programa malicioso. Nuestro análisis supone que Mydoom.b esta probablemente usando maquinas infectadas por el Mydoom original, lo que podría significar que son alrededor de 600,000 maquinas. Estas computadoras infectadas pudieron haber recibido un comando para enviar copias de Mydoom.b. Por lo tanto, la comunidad de computadoras puede estar enfrentando una epidemia mucho más seria que la causada por Mydoom.a el día 27 de Enero.

La nueva versión contiene mínimas innovaciones técnicas. Mydoom.b también se propaga por email y la red de archivos compartidos KaZaA. El email contiene en el cuerpo del mensaje un conjunto diferente de cadenas de texto. El archivo adjunto mide aproximadamente 28 KB y contiene la cadena de texto: "**sync-1.01; andy; I'm just doing my job, nothing personal, sorry**".

Mydoom.b esta programado para lanzar un ataque de Denegación de Servicio (DoS) entre el 1º de Febrero y el 12 Febrero de 2004 sobre dos sitios web: [www.sco.com](http://www.sco.com) y [www.microsoft.com](http://www.microsoft.com).

Además, el gusano modifica la operación del sistema para evitar que los usuarios accedan a la mayoría de los sitios de proveedores anti-virus, sitios relacionados con noticias de seguridad y varias secciones del sitio de Microsoft-

Una descripción detallada de Mydoom.b esta disponible en Kaspersky Virus Encyclopedia

## Nueva Tecnología de Actualizaciones

Las bases de datos de Kaspersky Anti-Virus ya han sido actualizadas con la protección contra Mydoom.b.

Kaspersky Lab cuenta con una nueva tecnología de actualización de base de datos de virus.

Esta nueva tecnología permite al usuario descargar en forma automática las actualizaciones de Kaspersky Antivirus a través de Internet cada **TRES HORAS**. A partir de las 12 Media noche, 3am, 6am, 9am, 12 Media Dia , 3pm, 6pm y 9pm

A diferencia de otras compañías Antivirus, Kaspersky Labs, realiza pruebas preliminares de las actualizaciones para evitar la posibilidad de falsas alarmas.

## Factores que permitieron la dispersión del Mydoom

A continuación se presentan los principales factores que permitieron la rápida epidemia de Mydoom:

1. **Ingeniería Social:** Este gusano enmascara los correos

infectados con correos que emulan errores comunes del sistema de correo, incitando a la gente a hacer clic sobre ellos. También, algunos de los adjuntos infectados son archivos comprimidos dentro de un ZIP, los cuales pueden parecer menos peligrosos para los usuarios.

2. **Zonas Horarias (Time zones):** A diferencia de la mayoría de otras epidemias recientes de gusanos de Internet, Mydoom fue encontrado a la mitad de horarios de oficina en USA y diferentes redes corporativas contrajeron inmediatamente la infección
3. **Colección agresiva de direcciones de correo:** Además de auto enviarse a las direcciones de correos encontradas de los archivos del usuario, el gusano también crea nuevas direcciones suponiendo nombres de usuarios comunes y los anexa al principio del nombre del dominio de las direcciones de correo encontradas. Esto también puede desviar algunos de los trucos que la gente utiliza para ocultar sus direcciones de correo de "basura" (spammers).

## Utileria para eliminar MyDoom

Kaspersky Labs ha liberado la versión 10.1.0.7 de su herramienta gratuita de limpieza automática CLRAV que incluye la desinfección de Mydoom y algunos otros virus.

Kaspersky Labs Herramienta de desinfección automática  
<http://avp.com.mx/descargas/utilerias/clrav.zip>

Kaspersky Lab Mexico  
Technical Support Department