El gusano informático Code Red fue descubierto aproximadamente el 13 de julio de 2001. Realizaba ataques a computadoras que trabajaran con el servidor web de Microsoft, Internet Information Server, IIS.

La empresa que descubrió y reportó este gusano fue eEye Digital Security, y aunque se reportó el 13 de julio, su extensión se llevó a cabo el 19 de julio, día en que los servidores infectados subieron en número a cerca de 359,000.

Funcionamiento

El gusano explotaba una vulnerabilidad en el indexado de la distribución de software IIS, que se encuentra descrita en el boletín MS01-033, sin embargo, en menos de un mes, el parche para solucionar este problema fue desarrollado.

El virus se extendía por medio de una vulnerabilidad comúnmente conocida como “buffer overflow”, en el archivo IDQ.DLL, utilizando una larga cadena de caracteres repetidos *n* veces hasta conseguir el desbordamiento de buffer, lo que permitía al gusano ejecutar código propio e infectar la máquina que había sido atacada.

La primera persona en descubrir cómo bloquear este gusano fue Kenneth D. Eichman, por lo que fue invitado a la Casa Blanca.

Cuando el gusano lograba infectar, incluía un aviso que indicaba que la máquina fue infectada:
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

Al acceder Code Red a una computadora vulnerable, examina la existencia del archivo C:\NOTWORM, creado por el mismo gusano para identificar si el equipo ya estaba infectado. En caso de no existir, el gusano seguía con la infección, de lo contrario, permanecía esperando la propagación por la red.

El gusano crea 100 threads simultáneos, lo que provocaba que el servidor colapsara y tuviera que ser reiniciado.
En caso de que la fecha actual del servidor estuviera entre el 20 y 28, el gusano intentaba un ataque de denegación de servicio a la dirección www.whitehouse.gov, mediante el envío de una gran cantidad de datos basura al puerto 80 y así colapsar los canales de comunicación.

En caso de que la fecha fuera después del día 28, los diferentes threads creados en la primera etapa de infección, quedaban en bucle infinito, causando inestabilidad y caída del servidor.

La novela

Este es el primer gusano sobre el que se ha escrito una novela, apoyada en fechas, la realidad del momento y los peligros, para enmarcar una teoría de conspiración y saber sobre los mayores secretos en aquel momento.