

LightEater Pone A Millones De BIOS En Riesgo

❌ Dos minutos es todo lo que se necesita este malware para destruir completamente un ordenador. En una presentación titulada «¿Cuántos millones de BIOS le gustaría que se infecten?» en CanSecWest conferencia de seguridad, los investigadores de seguridad **Corey Kallenberg** y **Xeno Kovah** revelaron que incluso una persona no calificada podría utilizar un implante llamado **LightEater** para infectar un sistema vulnerable en poco tiempo.

El ataque se podría utilizar para hacer que un ordenador quede inutilizable, pero también podría ser utilizado para robar contraseñas y datos de cifrado. El problema afecta a las placas base de empresas como Gigabyte, Acer, MSI, HP y Asus. Se ve agravada por las manufacturas para la reutilización de códigos a través de múltiples BIOS UEFI y usarlos en los usuarios domésticos, empresas y gobiernos en riesgo.

[The Register](#), Kovah explicó que el problema se agrava por el hecho de que muy pocas personas se toman la molestia de **actualizar la BIOS**. Esto es algo que el dúo espera cambiar, poniendo como factor de importancia la facilidad con que un BIOS sin parchear puede ser **infectado con el malware**.

En la presentación de la vulnerabilidad, Kallenberg y Kovah dijeron:

Así que crees que estás haciendo solo [OPSEC](#), ¿no? Vas a longitudes locas para protegerse, volver a instalar el sistema operativo principal cada mes, o el uso de un DVD en vivo consciente de la privacidad como [TAILS](#). Adivina qué? El malware de la BIOS no le importa!

El malware puede ser utilizado para infectar un gran número de

sistemas mediante la creación de SMM ([System Management Mode](#)), la cual se puede adaptar a las BIOS con una sencilla coincidencia de patrones. Un BIOS de Gigabyte se encontró que era particularmente inseguro.

Ni siquiera tenemos que hacer nada especial; acabamos de tener un controlador del núcleo escrito con una instrucción no válida a la primera instrucción de la CPU lee el chip flash, y bam, fue fuera de combate, y nunca fue capaz de arrancar de nuevo.

La vulnerabilidad es algo que ya ha sido explotado por la NSA, pero los investigadores están animando a las empresas y los gobiernos a tomar el tiempo para instalar los parches del BIOS, y así solucionar este problema de seguridad.