

NSA Encuentra Malware Oculto Durante Casi 20 Años En Discos duros

[Sigue el tablero Encuentra en nuestro blog! de HostDime en Pinterest.](#)

Cuando pensamos que el nivel de espionaje no puede tener un nivel intrusivo mayor del que hemos visto, se ha conocido sobre la **infección al firmware de los discos duros**. Ahora se ha descubierto que se ha estado usando este método para espiar a los objetivos durante casi 20 años.

Esta pieza de malware se usa mediante la **modificación del firmware del disco duro**, y [Kaspersky](#) dice que es compatible con casi todas las principales marcas de disco duro: Seagate, Western Digital, Samsung, lo que sea. Una vez que está **infectado el disco duro**, es casi imposible deshacerse o incluso detectar el malware. Ya que no ocupa espacio en los sectores del disco duro, puede fácilmente volver a infectar un sistema, incluso después de que la unidad ha sido completamente formateada.

Hay otro aspecto bastante sofisticado acerca de esta amenaza. **Kaspersky** descubrió que uno de sus objetivos era comprometer sistemas y redes con fallos. Hacer eso requiere no sólo el malware firmware residente, sino una herramienta complementaria que se entregó a través de una **unidad USB infectada**. La unidad comprometida se utilizó para transmitir comandos y recopilar información, con los datos enviados más tarde cuando fue conectado de nuevo en otro ordenador infectado con otro **componente de malware**.

El Malware es un componente avanzado, a pesar de esto, no tiene como objetivo equipos como el suyo y el mío (al menos eso es lo que estamos esperando, ¿verdad?). La lista de

objetivos según Kaspersky no le sorprenderá: instituciones gubernamentales y militares, de telecomunicaciones y empresas de energías, centros de investigación nuclear, compañías petroleras, desarrolladores de software de encriptación, medios de comunicación, grupos islámicos. La evidencia de los ataques se remonta a por lo menos 2001.

El [blog de Kaspersky](#) es muy detallado, ali se afirma que este malware **utiliza dos exploits** previamente desconocidos que luego se utilizaron en [Stuxnet](#), y ya se ha mostrado evidencia bastante fuerte que implican a los EE.UU. allí.