Un virus del tipo malware o software malicioso, que afecta al sistema operativo de Windows, iOS, Linux y BSD (distribución de software Berkeley), fue descifrado por el experto en seguridad Dragos Ruiu después de casi tres años sufriendo sus efectos.

El experto tardó todo este tiempo en descubrir por qué sus equipos se actualizaban solos y se conectaban a internet, incluso sin tener ninguna conexión habilitada.

Finalmente logró determinar que se trata de un malware que afecta directamente al BIOS (Sistema Básico de Entrada/Salida, por sus siglas en inglés) de la computadora, al que ha dado el nombre de 'badBIOS', y que conseguía interconectar unos equipos con otros a través de ultrasonidos, imposibles de detectar para el oído humano, que eran emitidos por los altavoces y detectados por los micrófonos de los equipos víctima.

Según Ruiu, el código malicioso actuó por primera vez en uno de sus ordenadores cuando después de la instalación de una versión reciente del sistema operativo iOS X en una MacBook Air, el equipo automáticamente decidió actualizar el firmware de la secuencia de arranque ('booting', en inglés), publica 'Ars Technica'.

Posteriormente el asesor en seguridad notó que desaparecían archivos y configuraciones sin motivo aparente y que le resultaba imposible 'bootear' desde un CD ROM. En los meses siguientes, este comportamiento comenzó a extenderse entre otros equipos en su red,

incluyendo algunos con Open BSD y múltiples variantes de Windows.

"Fue como, bueno, estamos totalmente dominados" declaró Ruiu a 'Ars Technica'. "Tenemos que borrar todos nuestros sistemas y empezar de cero, lo cual hicimos. Fue un ejercicio muy doloroso. He estado sospechando de todos los objetos por aquí desde entonces".

Ruiu empezó entonces una lucha de casi tres años para eliminar el malware. Durante este tiempo intentó de todo, hasta reinstalar los sistemas operativos desde cero y sobre discos duros nuevos, pero el malware parecía 'inmortal'.

El virus hace que los aparatos que se encuentran en un radio moderado comiencen a transmitirse paquetes de datos entre sí. Por ese motivo decidió aislar completamente los equipos, desconectando el cable Ethernet, removiendo las tarjetas wifi y bluetooth y desconectándolos de la red eléctrica, trabajando con baterías, pero la transmisión de paquetes continuaba y el virus seguía propagándose. El último recurso de Ruiu fue remover las bocinas internas y el micrófono de un equipo, lo cual acabó con la transmisión de paquetes.

Este sistema de envío de información a través de sonidos de alta frecuencia ya ha sido objeto de investigación en varios laboratorios, incluyendo un proyecto que lleva a cabo el MIT.

A pesar del escepticismo que rodea el anuncio del potente virus, no es la primera vez que un código malicioso aparece contenido en el firmware. Se tiene el caso de Stuxnet, el virus que afectó al control de las centrifugadoras de enriquecimiento de uranio iraníes hace unos años.