Una de las compañías más importantes de telecomunicaciones en Estados Unidos, descubrió hardware manipulado de Super Micro Computer Inc. en su red y lo eliminó en agosto pasado, lo que serviría de evidencia sobre la reciente manipulación en China de componentes electrónicos críticos con destino a Estados Unidos, según un experto que trabaja para la compañía de telecomunicaciones.

Bloomberg publicó dicha información en su sitio web, respaldando su anterior historia que ha sido duramente criticada por el gobierno de Estados Unidos y las compañías del mismo país.

Yossi Appleboum, experto en seguridad, proporcionó documentos, análisis y otras pruebas sobre el descubrimiento después de la publicación de un informe en Bloomberg Businessweek que dice cómo los servicios de inteligencia de China ordenaron a subcontratistas la implantación de chips maliciosos en las tarjetas madre de los servidores Supermicro durante un periodo de dos años, periodo que terminó en 2015.

Appleboum trabajó en la unidad de tecnología del Cuerpo de Inteligencia del Ejército Israelí, y ahora es director ejecutivo de Sepio Systems, en Gaithersburg, Maryland.

Su compañía se especializa en seguridad de hardware, fue contratada para escanear diversos centros de datos grandes que pertenecen a la compañía de telecomunicaciones.

Las comunicaciones inusuales de un servidor Supermicro y una posterior inspección física, han revelado que se manipuló el conector Ethernet del servidor, dijo Appleboum.

También aseguró que ha visto manipulaciones similares de hardware en computadoras de distintos fabricantes hechas por contratistas en China, y no sólo de productos de Supermicro.

«Supermicro es una víctima, al igual que todos los demás», dijo. Agregó que existen innumerables puntos en la cadena de suministro en China, donde se puede realizar manipulaciones y percatarse puede ser imposible en muchos casos. *«Ese es el problema con la cadena de suministro china»*, dijo.

> Supermicro con sede en San José, California, dijo: *«La seguridad de nuestros clientes y la integridad de nuestros productos son fundamentales para nuestro negocio y los valores de nuestra compañía. Nos encargamos de garantizar la integridad de nuestros productos durante todo el proceso de fabricación, y la seguridad de la cadena de suministro es un tema muy importante para nuestra industria. Aún no tenemos conocimiento sobre ningún componente no autorizado y ningún cliente nos ha informado que se encontraron dichos componentes. Estamos consternados de que Bloomberg solo nos de información limitada, sin documentación y sólo medio día para responder a estas nuevas acusaciones».*

Bloomberg asegura que contactó por primera vez a Supermicro para comentar sobre el reportaje el lunes a las 9:23 am, hora del este, y le dio a la compañía 24 horas para responder.

Respecto al reportaje anterior de Bloomberg, Supermicro dijo que *«refuta enérgicamente»* los informes sobre supuestos chips maliciosos en los servidores que vendió a los clientes. Mientras tanto, la embajada de China en Washington, no respondió a la solicitud de comentarios el lunes.

Debido a todo este problema, las acciones de Supermicro cayeron un 41% el pasado jueves, siendo la peor caída desde que se convirtió en una empresa pública en 2007.

Según los informes de Bloomberg, la implantación de chips está diseñada para brindar a los atacantes acceso invisible a los datos en una red de computadoras en la que está instalado el servidor. Se descubrió que las alteraciones se hicieron en la fábrica cuando la placa base estaba siendo producida por un subcontratista de Supermicro en China.

Appleboum inspeccionó uno de los dispositivos en cuestión y determinó que el servidor de la compañía de telecomunicaciones fue modificado en la fábrica donde se manufacturó. Aseguró que los contactos de inteligencia occidentales le dijeron que el dispositivo se fabricó en un lugar con subcontratistas de Supermicro en Guangzhou, una ciudad portuaria en el

sureste de China.

Guangzhou, que está a unas 90 millas de Shenzhen, es considerado como el Silicon Valley del Hardware, donde se encuentran empresas grandes como Tencent Holdings Ltd. y Huawei Techonologies Co. Ltd.

El hardware manipulado fue encontrado en una instalación que tenía muchos servidores de Supermicro, los técnicos de la compañía de telecomunicaciones no han podido responder qué tipo de datos se utilizaban en el servidor infectado. Appleboum estuvo presente en una inspección visual de dicho servidor. Aún no se sabe si la compañía de telecomunicaciones contactó al FBI sobre este hallazgo.

Otras compañías han informado que no están al tanto de lo sucedido. Fletcher Cook, portavoz de AT&T Inc., dijo que *«estos dispositivos no forman parte de nuestra red, y no estamos afectados».* Un portavoz de Verizon Communications Inc., afirmó que *«no estamos afectados».*

Las redes de comunicaciones de Estados Unidos han sido objetivo importante de agencias de inteligencia extranjeras, ya que los datos de millones de teléfonos celulares, computadoras y otros dispositivos pasar por medio de sus sistemas. Los implantes de hardware son herramientas clave que se usan para tener acceso secreto a dichas redes, realizar reconocimientos y buscar la propiedad intelectual corporativa o secretos gubernamentales.

La manipulación del conector Ethernet antes mencionada, parecía ser similar al método utilizado por la Agencia de Seguridad Nacional de Estados Unidos, cuyos detalles fueron filtrados en 2013. En correos electrónicos, Appleboum y su equipo aseguran que anteriormente habían visto algunas variaciones en las investigaciones de hardware hechas por otras compañías que fabrican en China.

Es muy difícil poder detectar manipulación de hardware, por lo que las agencias de inteligencia invierten miles de millones de dólares en este tipo de sabotaje. Según Bloomberg, Estados Unidos cuenta con grandes programas de tecnología que se dirigen a

países extranjeros mediante implantes de espionaje, información basada en las revelaciones del ex empleado de la CIA, Edward Snowden.

Tres expertos en seguridad analizaron implantes de hardware extranjeros para el Departamento de Defensa de Estados Unidos, confirmando que la forma en que el software Sepio detectó el implante es bastante confiable.

En el caso de la compañía de telecomunicaciones, la tecnología de Sepio ha detectado que el servidor Supermicro manipulado aparecía en la red como dos dispositivos en uno solo. El servidor legítimo se comunicaba de una forma y el implante de otra, pero todo el tráfico parecía provenir del mismo servidor de confianza, por lo que logró pasar por los filtros de seguridad.

Appleboum afirmó que un signo clave del implante, es que el conector Ethernet manipulado cuenta con lados metálicos en lugar de plásticos habituales. El metal es necesario para poder disipar el calor del chip escondido en el interior, que actúa como una mini computadora.

> *«El módulo parece realmente inocente, de alta calidad y original, pero se agregó como parte de un ataque a la cadena de suministro»,* dijo.

El objetivo de dichos implantes de hardware es establecer un área de almacenamiento encubierta dentro de redes sensibles, según Appleboum y su equipo. Aseguran que esto representa una grave infracción de seguridad, por lo que alertaron al equipo de seguridad del cliente en agosto pasado, mismo que los eliminó después del análisis.

La amenaza de los implantes de hardware es *«demasiado real»,* dijo Sean Kanuck, quien fue hasta 2016 el principal funcionario cibernético dentro de la Oficina del Director de Inteligencia Nacional. Ahora es director de conflictos futuros y seguridad cibernética para el Instituto Nacional de Estudios Estratégicos en Washington.

> *«Los fabricantes que pasan por alto esta preocupación están ignorando un problema potencialmente grave», dijo Kanuck. «Los ciberactores capaces, como los servicios de inteligencia y seguridad chinos, pueden ser capaces de acceder a la cadena de suministro de TI en múltiples puntos para crear subversiones avanzadas y persistentes».*

Un punto clave de cualquier ataque de hardware exitoso es la alteración de los componentes que cuentan con una fuente de alimentación amplia, siendo este un desafío al adentrarse en una placa madre. Por esto, los periféricos como los teclados y ratones, también son los favoritos para las agencias de inteligencia, aseguró Appleboum.

Gracias a los informes de Bloomberg sobre el ataque contra productos de Supermicro, grandes empresas, bancos y proveedores de computación han estado analizando sus servidores y demás hardware para comprobar si existen modificaciones.

Expertos en seguridad nacional aseguran que un problema grave es que para tratarse de una industria de seguridad cibernética que se acerca a los 100 mil millones de dólares anuales, se ha gastado muy poco en inspección de hardware, lo que ha permitido a las agencias de inteligencia de todo el mundo trabajar sin impedimentos, especialmente en China.

> *«Para China, estos esfuerzos abarcan todo»,* afirmó «Tony Lawrence, CEO de VOR Technology. *No hay forma de que podamos identificar la gravedad o el tamaño de dichas acciones, no lo sabremos hasta que encontremos alguna. Podría estar por todas partes, podría ser cualquier cosa que salga de China. Lo desconocido es lo que te atrapa y ahí es donde estamos ahora. No conocemos el nivel de explotaciones dentro de nuestros propios sistemas».*