



Encuentran chips de espionaje en servidores de grandes compañías como Amazon y Apple

Un reporte ha revelado detalles sobre un ataque a cadenas de suministro, siendo uno de los programas corporativos de espionaje y piratería de hardware más grande de los últimos tiempos.

Según un informe publicado por Bloomberg, se encontró un pequeño chip de vigilancia, no más grande que un grano de arroz, oculto en los servidores utilizados por unas 30 compañías estadounidenses, entre ellas, Apple y Amazon.

Dichos chips no forman parte de las tarjetas madre del servidor original diseñadas por la empresa Super Micro, de Estados Unidos, estos chips se habían añadido durante el proceso de fabricación en China.

En el informe basado en una investigación secreta de 3 años en Estados Unidos, se detalla que los grupos afiliados al gobierno chino lograron infiltrarse en la cadena de suministro para instalar los microchips de vigilancia en las placas base que se convirtieron en servidores desplegados por el ejército de Estados Unidos, agencias de inteligencia del mismo país y muchas empresas.

«Apple ha descubierto chips sospechosos dentro de los servidores de Supermicro alrededor de mayo de 2015, luego de detectar una actividad de red extraña y problemas de firmware, según una persona familiarizada con la compañía», dice el informe.

«Dado que los implantes eran pequeños, la cantidad de código que contenían también era pequeña. Pero fueron capaces de hacer dos cosas importantes: decirle al dispositivo que se comuniquen con una de varias computadoras anónimas en otro lugar de Internet que se cargaron con más código complejo, además de preparar al sistema operativo para aceptar el nuevo código».

Se sospecha que los chips fueron agregados para ayudar al gobierno chino a espiar a las compañías estadounidenses y sus usuarios. Básicamente, *«se trata de un hackeo de*



Encuentran chips de espionaje en servidores de grandes compañías como Amazon y Apple

hardware» que según la publicación, «es más difícil de lograr y potencialmente más devastador, prometiendo el acceso a largo plazo a las agencias que han invertido millones de dólares y muchos años para obtener la información».

«Dependiendo del modelo de la tarjeta, los chips varían en tamaño, sugiriendo que los atacantes suministraron diferentes lotes en las fábricas», dice el reporte.

La publicación también afirma que Apple y Amazon encontraron los chips en sus servidores en 2015 y reportaron a las autoridades de Estados Unidos, aunque Apple y Amazon refutaron fuertemente dichas afirmaciones.

Apple dijo a Bloomberg que la compañía nunca encontró chips maliciosos, «manipulación de hardware» o vulnerabilidades plantadas a propósito en sus servidores, tampoco «tuvieron ningún contacto con el FBI o cualquier otra agencia sobre dicho incidente».

Apple terminó su relación con Super Micro en 2016. La compañía informó que los reporteros de Bloomberg confundieron la historia con un accidente previo de 2016 en el que la compañía encontró un controlador infectado en un servidor Super Micro en sus laboratorios.

«Si bien no existió ninguna reclamación de que los datos de los clientes fueron involucrados, tomamos estas alegaciones con seriedad y queremos que los usuarios sepan que hacemos todo lo posible por salvaguardar la información personal que nos confían», dijo Apple. «También queremos que sepan que lo que Bloomberg informa sobre Apple es inexacto».

Amazon por su parte también afirma que es falso que la compañía supiera de un compromiso de la cadena de suministro, o de «servidores que contienen chips maliciosos o modificaciones en centros de datos con sede en China».



Encuentran chips de espionaje en servidores de grandes compañías como Amazon y Apple

Por su parte, SuperMicro y el Ministerio de Relaciones Exteriores de China han negado enérgicamente los hallazgos de Bloomberg. [Aquí se puede encontrar una lista oficial](#) sobre las declaraciones oficiales de Amazon, Apple, SuperMicro y el Ministerio de Asuntos Exteriores de China.