Hackers atacaron y comprometieron a *«cientos de miles»* de propietarios de computadoras Asus al utilizar una herramienta de software de actualización con una puerta trasera desde los propios servidores de la compañía.

Motherboard informó por primera vez lo sucedido, asegurando que los piratas informáticos firmaron digitalmente la herramienta Asus Live Update con uno de los certificados de firma de código propios de la compañía antes de enviarlo a los servidores de descarga de Asus, mismo que albergó la herramienta de *«backdoor»* durante varios meses el año pasado.

Las actualizaciones maliciosas se enviaron a las computadoras Asus, que cuentan con el software instalado de forma predeterminada.

TechCrunch confirmó muchos de los informes de Motherboard luego de enterarse del ataque hace algunas semanas de una fuente con conocimiento directo del incidente.

Kasperskey encontró el software de puerta trasera y aseguró que la herramienta de actualización maliciosa podría afectar a más de un millón de usuarios. La puerta trasera escanearía un dispositivo en busca de la dirección MAC única de un objetivo y extraer una carga maliciosa de un servidor de comando y control.

Sin embargo, aún no se sabe exactamente qué carga útil se entregó a las víctimas.

Los informes de Motherboard indican que la puerta trasera estaba escaneando unas 600 direcciones MAC, y probablemente estaba dirigida a infectar solo a un pequeño número de víctimas en lugar de causar infecciones a gran escala.

Symantec confirmó los hallazgos de Kaspersky y los describió como un ataque de cadena de suministro de software.

> *«Nuestros hallazgos sugieren que la versión trojanizada del software se envió a los clientes de ASUS entre junio y octubre»*, informó Jennifer Duffourg, portavoz de la

> compañía.

La compañía de seguridad también dijo que vio el software de puerta trasera implementado entre junio y fines de octubre de 2018, que afectó a 13,000 de sus clientes.

Se cree que los piratas informáticos tuvieron acceso a los certificados propios de Asus para firmar el malware por medio de la extensa cadena de suministro de Asus, una línea de factor de desarrolladores y proveedores de todo el mundo en los que se confía para desarrollar software y proporcionar componentes para las computadoras de Asus.

Estos ataques a la cadena de suministro son muy difíciles de detectar ya que por lo regular involucran el ataque a una empresa con información privilegiada o infiltrarse directamente en la compañía.

Uno de los archivos de puerta trasera utilizó un certificado creado a mediados de 2018 pero que era diferente de los certificados que usaba Asus regularmente.

Según el informe de Motherboard, los certificados siguen activos y no han sido revocados, lo que representa un enorme riesgo para los clientes de Asus.

La puerta trasera tiene un parecido con CCleaner, que de forma similar utiliza un certificado de firma de código para ocultar cualquier componente malicioso. Cerca de 2.3 millones de clientes se vieron afectados por dicha puerta trasera.

Asus por su parte, no ha informado a los clientes acerca de la vulnerabilidad luego de ser descubierta a inicios de este año.

Motherboard informó que Kaspersky emitió información sobre el software de puerta trasera el 31 de enero. Asus, con sede en Taiwán, cuenta con el 6% del mercado de computadoras, según Gartner, que envía millones de computadoras al año.

Hasta el momento Asus no ha respondido a solicitudes de comentarios y Sarah Kitsos, de Kaspersky, tampoco ha hecho comentarios sobre los hallazgos.