Andres Freund, el ingeniero que previno un posible ciberataque global

Tiempo de lectura: 5 min.
Kevin Roose

Cualquiera que trabaje a fondo en las trincheras de internet te dirá que no es una maquinaria bien aceitada que funcione sin el menor problema.

Más bien, es un conjunto de partes desorganizadas que se han ido ensamblando a lo largo de décadas y que solo se mantienen juntas gracias al equivalente digital de una cinta adhesiva y goma de mascar. Gran parte de la red depende de software de código abierto que se mantiene por el trabajo de un pequeño ejército de programadores voluntarios a quienes nadie les da las gracias por reparar los errores, parchar los huecos y asegurarse de que ese artilugio desvencijado, que maneja billones de dólares en producto interno bruto global pueda, a duras penas, seguir andando.

Es muy probable que la semana pasada uno de esos programadores haya salvado a internet de un enorme problema.

Su nombre es Andres Freund. Es un ingeniero de software de 38 años que vive en San Francisco y trabaja para Microsoft. Parte de su trabajo consiste en desarrollar una porción de software de código abierto para gestionar bases de datos conocido

como PostgreSQL. Si pudiera explicar correctamente de qué se trata este software (algo que, en definitiva, no puedo hacer), quizá solo lograría matarlos de aburrimiento.

Hace poco, mientras realizaba algunas tareas rutinarias de mantenimiento, Freund descubrió sin querer una puerta trasera oculta en un fragmento de software que forma parte del sistema operativo de Linux. Es posible que esa puerta trasera haya sido el preludio de un importante ataque cibernético que, en opinión de los expertos, podría haber ocasionado daños terribles de haberse concretado.

Ahora, en un giro digno de Hollywood, varios líderes de la industria tecnológica e investigadores de ciberseguridad están calificando a Freund de héroe. Satya Nadella, director ejecutivo de Microsoft, elogió su “curiosidad y destreza”. Un admirador lo describió como “el gorila líder de los nerdos”. Entre los ingenieros ha estado circulando una vieja tira cómica de la web, famosa entre los programadores, cuya premisa es que toda la infraestructura digital moderna depende de un proyecto mantenido por un tipo cualquiera en Nebraska (según ellos, Freund es ese tipo).

En una entrevista realizada esta semana, Freund —quien en realidad es un programador nacido en Alemania de voz suave que no quiso que le tomaran una fotografía para este artículo— comentó que convertirse en un héroe popular en internet le ha causado gran confusión.

“Se me hace muy extraño”, dijo. “Soy una persona bastante reservada que solo se sienta frente a la computadora y produce código”.

La saga inició este mismo año, durante un vuelo de Freund de regreso a casa después de visitar a sus padres en Alemania. Mientras revisaba un registro de pruebas automatizadas, se percató de que había unos cuantos mensajes de error que no reconocía. En ese momento sufría los efectos del desfase horario y los mensajes no parecían urgentes, así que los archivó en su memoria.

Pero unas semanas después, mientras realizaba otras pruebas en casa, observó que una aplicación llamada SSH, que se utiliza para ingresar de manera remota a las computadoras, consumía más potencia de procesamiento de lo usual. Después de buscar el origen del problema, que rastreó hasta un conjunto de herramientas de compresión de datos llamadas xz Utils, se preguntó si estaría relacionado con los errores que había visto antes.

(No se preocupen si con estos nombres les parece que hablo en chino; en realidad, solo necesitan saber que son pequeños fragmentos del sistema operativo de Linux, que quizá sea el software de código abierto más importante del mundo. La gran mayoría de los servidores del mundo —incluidos los que utilizan los bancos, los hospitales, el gobierno y las empresas de la lista Fortune 500— operan con Linux, por lo que su seguridad es de importancia global).

Al igual que otros softwares populares de código abierto, Linux se actualiza con frecuencia y la mayoría de los errores se deben a equivocaciones inocentes. Sin embargo, cuando Freund examinó con más detenimiento el código fuente de xz Utils, encontró pistas que indicaban que alguien lo había alterado de manera intencional.

En particular, descubrió que alguien había sembrado código maligno en las versiones más recientes de xz Utils. El código, conocido como una puerta trasera, le permitiría a su creador secuestrar la conexión SSH de un usuario y correr en secreto su propio código en la máquina de ese usuario.

En un primer momento, Freund dudó de sus hallazgos. ¿De verdad había descubierto una puerta trasera en uno de los programas de código abierto más analizados del mundo?

“Sentí que era surreal”, relató. “Pensé varias veces que tal vez había dormido mal y estaba delirando”.

Pero conforme siguió analizando, identificó pruebas nuevas, así que la semana pasada Freund compartió sus hallazgos con un grupo de desarrolladores de software de código abierto. La noticia no tardó en causar alarma en el mundo tecnológico. En solo unas horas, se creó una reparación y algunos investigadores le dieron crédito a Freund por haber evitado un ciberataque que podría haber sido histórico.

Nadie sabe quién sembró la puerta trasera pero, al parecer, el plan era tan elaborado que algunos investigadores están convencidos de que solo podría haberlo intentado una nación con habilidades tremendas para concebir ataques cibernéticos, como Rusia o China.

Según algunos investigadores que han revisado la evidencia, todo parece indicar que el atacante utilizaba un pseudónimo, “Jia Tan”, para sugerir cambios a xz Utils desde incluso 2022 (muchos proyectos de software de código abierto se rigen

mediante un sistema jerárquico; los desarrolladores proponen cambios al código de un programa, y luego los programadores más experimentados se encargan de revisar y aprobar los cambios).

Se cree que el atacante, utilizando el nombre Jia Tan, trabajó varios años para ganarse poco a poco la confianza de otros desarrolladores de xz Utils y obtener más control sobre el proyecto, hasta que ascendió en la jerarquía interna y, finalmente, insertó el código con la puerta trasera oculta este mismo año (aunque la nueva versión manipulada del código ya se había dado a conocer, todavía no era de uso generalizado).

Freund señaló que, desde que sus hallazgos se hicieron públicos, se ha dedicado a ayudar a los equipos que intentan reproducir el ataque con ingeniería inversa para identificar al culpable. Así que ha estado muy ocupado para dormirse en sus laureles. La siguiente versión de PostgreSQL, el software de gestión de bases de datos en el que trabaja, saldrá más adelante este mismo año y Freund todavía busca que se acepten algunos cambios de último minuto antes de la fecha límite.

“En realidad, no tengo tiempo de ir a tomar unos tragos para celebrar”, dijo.

5 de abril 2024

The Times

https://www.nytimes.com/es/2024/04/05/espanol/andres-freund-ciberataque-global.html