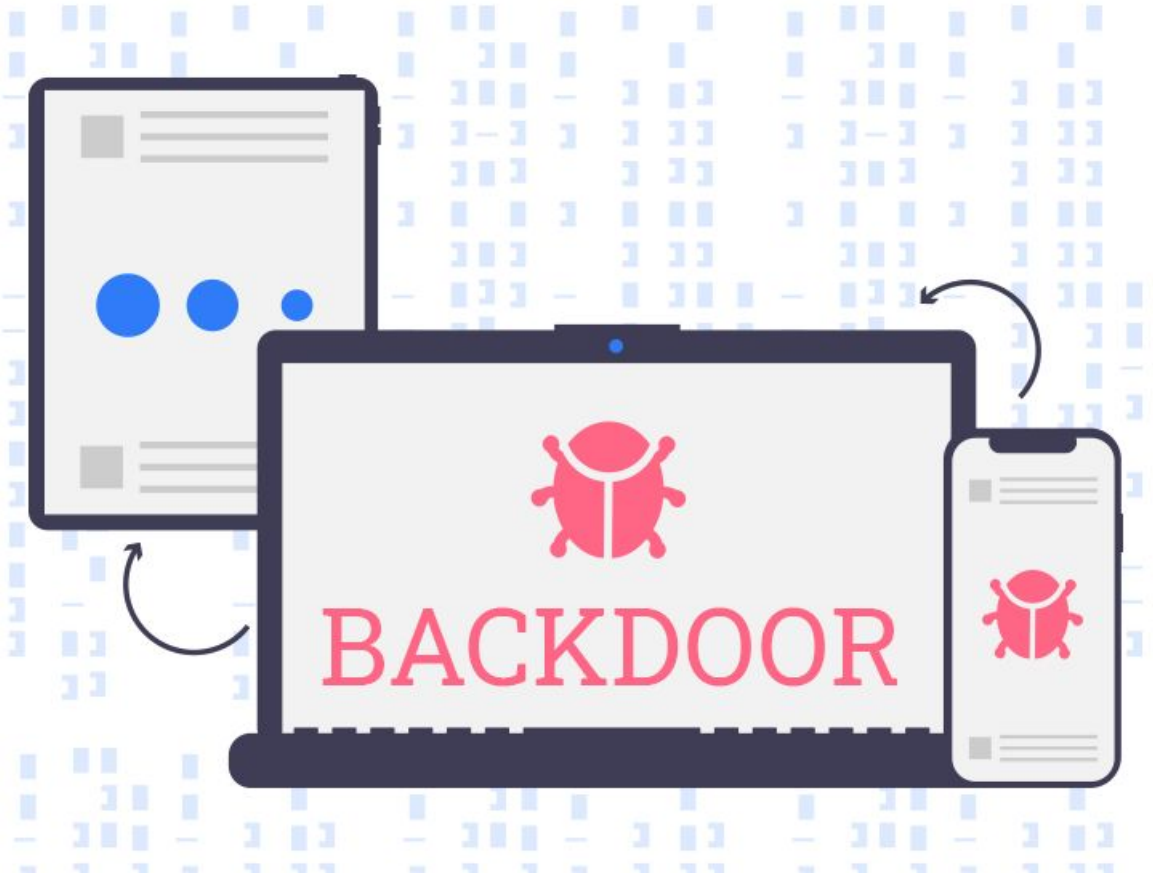
Ataque a la cadena de suministros de XZ

Armando Cruz Maldonado
Díaz González Rivas Ángel Iñaqui

Introducción

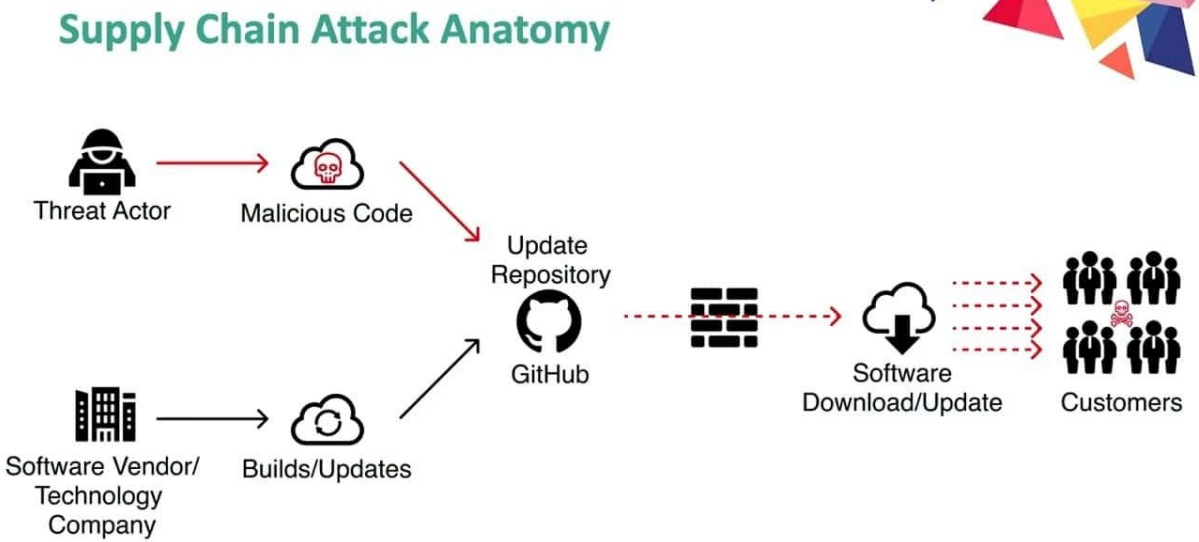
Ataques a Cadenas de Suministro: Son ciberataques dirigidos a proveedores externos cuyo software o servicios son vitales en la cadena de suministro de una organización. Estos ataques se aprovechan del eslabón más débil en lugar de atacar directamente a la organización principal

Backdoors: son métodos de acceso no autorizado que permiten a los atacantes tomar el control de sistemas o dispositivos de manera encubierta.



Introducción

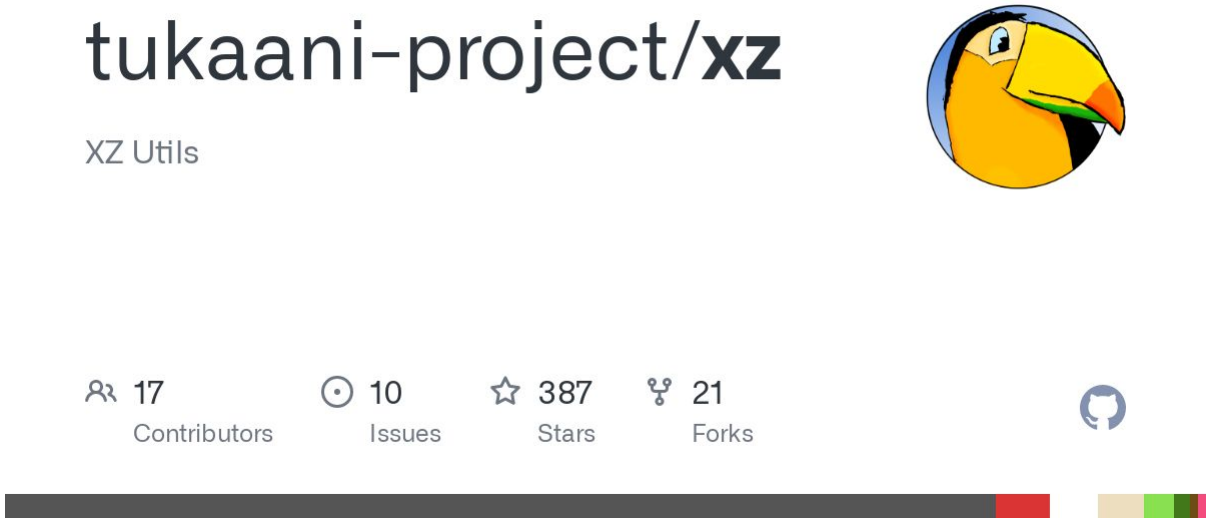
Las cadenas de suministro son extensas y a menudo difíciles de rastrear, lo que las hace vulnerables a ataques. Las organizaciones que dependen de servicios de terceros, especialmente en el ámbito digital, están expuestas a estos riesgos.



Tukaani

Tukaani busca crear una distribución de Linux basada en Slackware que quepa en un solo CD-ROM (disco compacto de solo lectura)

Tukaani es a donde reside xz-utils el cual era dirigido por Lasse Collin y Jia Tan hasta que fue removido el 31 de marzo de 2024



XZ

- XZ Utils es una evolución en la compresión de datos basada en el algoritmo de cadenas de Markov/Lempel-Ziv.
- Proporciona una alta tasa de compresión, aunque a costa de un mayor uso de memoria.
- Es ampliamente utilizado y está presente en la mayoría de las distribuciones de Linux.

El ataque

- En marzo de 2024, Andrés Freund descubrió un ataque a la cadena de suministro que afectó a XZ Utils.
- Afectó a las versiones 5.6.0 y 5.6.1 y a las distribuciones que tengan contenida a glibc
- El ataque se materializó a través de archivos de prueba maliciosos.
- El ataque se originó a partir de un backdoor introducido por Jia Tan, un desarrollador de XZ Utils.

Naturaleza del Ataque

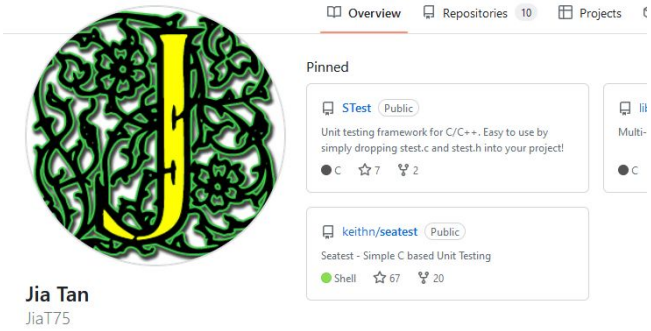
- El código malicioso se inyectaba en los archivos prueba de XZ Utils, específicamente en "tests/files/bad-3-corrupt_lzma2.xz" y "tests/files/good-large_compressed.lzma".
- Inserción de un script malicioso durante la compilación.
- Explotación de vulnerabilidades en sistemas x86-64 Linux.
- Activación de la backdoor y el potencial acceso remoto y control de sistemas infectados.

Naturaleza del Ataque

- La seguridad en conexiones SSH.
- Los atacantes podrían haber utilizado el backdoor para robar datos, instalar malware o realizar otros ataques.

CAUSAS

2021 creación de cuenta de Jia Tan en github



2022 Jia Tan hace su primer commit en XZ

se vuelve contribuyente regular de XZ

CAUSAS

2023 correo electrónico en oss-fuzz de Google se actualizó para ser el de Jia

2024 cambio la URL del proyecto de tukaani.org/xz/

paso a xz.tukaani.org/xz-utils/.

CAUSAS

Andres Freund descubrió las inconsistencias en los procesos de SSHD.

github cierra las cuentas de Jia Tan y Lasse Colin.

La cuenta de colin está activa además de que está restaurando los cambios que hizo Jia Tan

SSHD

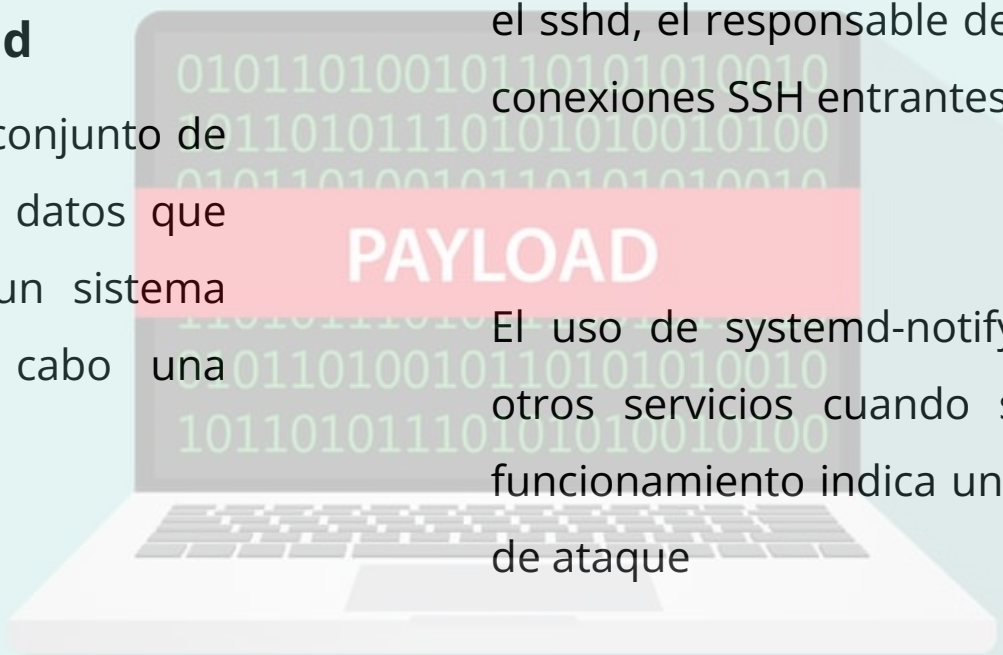
Se encarga de administrar las conexiones SSH entrantes y facilitar la autenticación de usuarios remotos y la comunicación segura entre sistemas

sandbox

se refiere a un entorno de ejecución restringido y controlado que se utiliza para ejecutar aplicaciones de forma segura y aislada del sistema operativo subyacente.

Payload

se refiere a un conjunto de instrucciones o datos que se cargan en un sistema para llevar a cabo una tarea específica



La payload se carga indirectamente en el sshd, el responsable de gestionar las conexiones SSH entrantes.

El uso de systemd-notify para iniciar otros servicios cuando sshd está en funcionamiento indica una posible ruta de ataque

Ejemplificación a un ataque RCE

- Proceso de verificación:

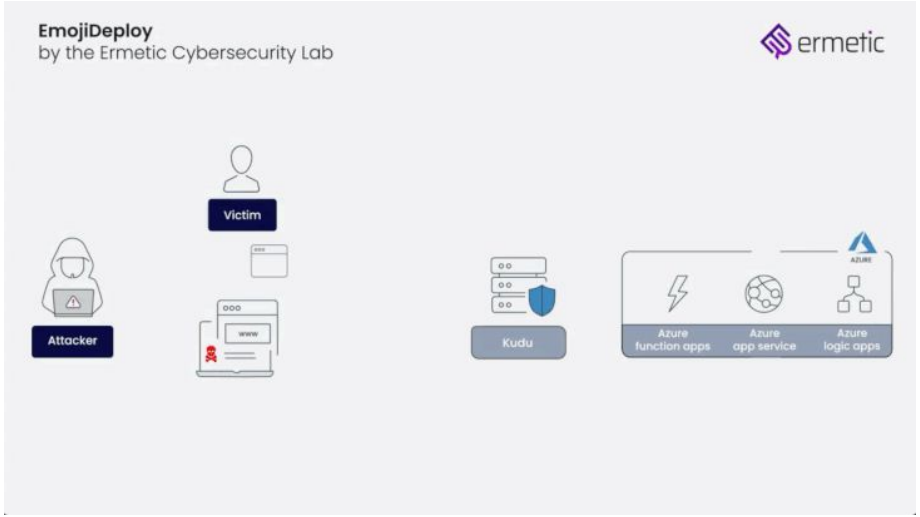
  función llamada “RSA_public_decrypt.” , firma digital llamada “Ed448”, clave fija llamada “ChaCha20”

- Proceso de descifrado:

  Verificación de autenticidad

- Proceso de autentificación:

  cifrado asimetrico, certificados OpenSSH

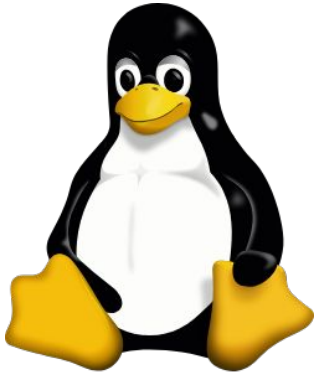


CMake

es una herramienta de código abierto, utilizada para automatizar el proceso de construcción de software

Landlock

Es un mecanismo de seguridad de linux, permite a los usuarios y aplicaciones imponer restricciones de acceso al sistema de archivos



Valoración

¿porque fue considerado un ataque significativo?

- Forma que fue descubierto
- afectaciones al equipo infectado
- Cantidad de usuarios que utilizan distribuciones de linux

Referencias

- James, J. (2024). FAQ on the xz-utils backdoor (CVE-2024-3094). GitHub Gist. https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27
- Boehs, E. (2024, Marzo 29). Everything I know about the XZ backdoor. Recuperado el 19 de abril del 2024, de https://boehs.org/node/everything-i-know-about-the-xz-backdoor#fnref2
- Collin, L. (2024). XZ Utils backdoor. https://tukaani.org/xz-backdoor/
- Valsorda, F. [@filippo.abyssdomain.expert]. (2024, 30 de marzo). I'm watching some folks reverse engineer the xz backdoor, sharing some *preliminary* analysis with permission. The hooked RSA_public_decrypt. Bluesky Social. https://bsky.app/profile/filippo.abyssdomain.expert/post/3kowjkx2njy2b
- Freund, A. (2024, 29 de marzo). [oss-security] backdoor in upstream xz/liblzma leading to ssh server compromise. LWN.net. https://lwn.net/ml/oss-security/20240329155126.kjjfduxw2yrlxgzm@awork3.anarazel.de/

Referencias

- Debian Webmaster, webmaster@debian.org. (s. f.). Debian -- Details of package xz-utils in sid. https://packages.debian.org/es/sid/xz-utils
- Developers, T. L. (s. f.). The Tukaani project. © the Tukaani Project. https://ftp.uni-bayreuth.de/packages/tools/lzma/tukaani.org/
- Read-McFarland, A.(2023, Mayo 11). ¿Qué es un Ataque a la Cadena de Suministros? Todo lo que deben saber las empresas. Wildix Blog. https://blog.wildix.com/es/que-es-un-ataque-a-la-cadena-de-suministros/
- Gómez, J. A. (2024, Febrero 2). Backdoor o Puerta Trasera: Qué es, Cómo Evitarlos y Eliminarlos. https://www.deltaprotect.com/blog/backdoor-o-puerta-trasera
- Communications. (2023, Diciembre 28). Cómo afectan las “backdoor” o puertas traseras en tus dispositivos. BBVA NOTICIAS. https://www.bbva.com/es/innovacion/como-afecta-las-backdoor-o-puertas-traseras-en-tus-dispositivos/

Referencias

- WinZip | Download your free Trial. (s. f.). https://www.winzip.com/es/learn/file-formats/tar/
- Análisis Irontec ataque xz Utils herramienta distribuciones Linux. (2024, April 12). Irontec - Consultoría Tecnológica. https://www.irontec.com/news/analisis-irontec-ataque-xz-utils-herramienta-distribuciones-linux
- Vargas, R. (s. f.). Archivos .TAR. . . ¿Qué son? ¿Cómo usarlos? - RicardoVargas.me. https://ricardovargas.me/es/bitacora-web/articulos/item/archivos-tar-que-son-como-usarlos
- Valgrind home. (s. f.). https://valgrind.org/
- Micucci, M. (2024, 2 de febrero). La ofuscación de código: un arte que reina en la ciberseguridad. welivesecurity. https://www.welivesecurity.com/es/recursos-herramientas/ofuscacion-de-codigo-arte-ciberseguridad/
- ¿Qué es SSH? Definición y detalles. (s. f.). https://www.paessler.com/es/it-explained/ssh