

Software Supply-Chain Attacks

Hashdump Security Club

Software supply chain attacks

- **Type of cyberattack that exploits weaknesses within third parties**
- **By compromising a dependency (e.g. a library or software repository), malware can be planted within an organization**
- **Through this method, the weakest link can be targeted**
  - Has become an increasingly common threat
- **Can exploit the human element of software development**
  - The volunteer nature of much open-source development makes it a vulnerable target

SolarWinds hack

- **One of the most famous software supply chain attacks**
- **18,000+ SolarWinds customers received malicious builds**
  - Included government agencies such as the Cybersecurity and Infrastructure Agency (CISA)
- **Malware injected into Orion network monitoring software**
  - Rather than modifying source code, attackers slipped malware into software builds
- **Positioning within security software gave malware access to large number of machines**
- **Disguised network traffic as standard Orion protocol to avoid detection**



https://commons.wikimedia.org/wiki/File:Official_SolarWinds_Logo.svg

npm

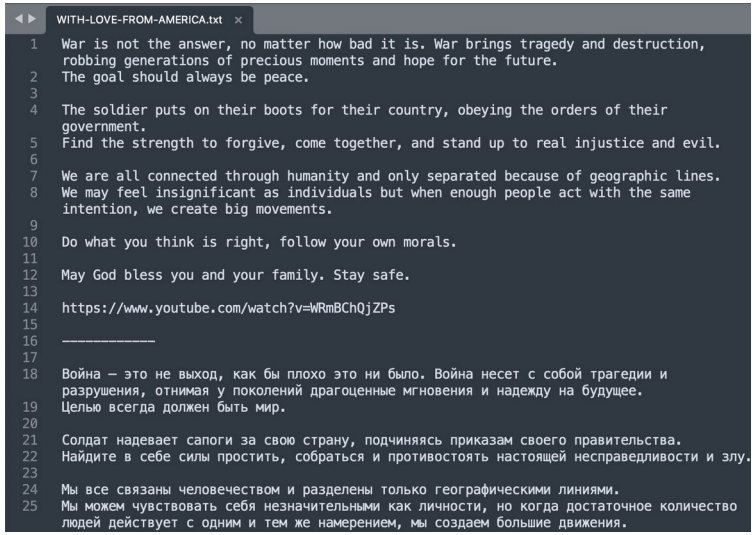
- **Most common package manager for JavaScript and TypeScript**
- **Has an online repository of open-source software libraries**
- **These packages are user-submitted**
  - Not validated by a central authority
- **Unverified nature has led to exploitation in supply-chain attacks**
  - Even in ecosystems detached from JS or TS



https://commons.wikimedia.org/wiki/File:Npm-logo.svg

peacenotwar

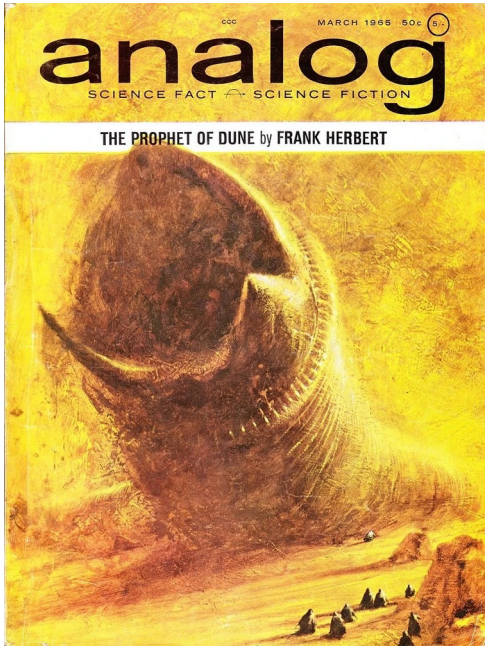
- **March 2022: the widely-used node-ipc package on npm is updated**
  - New dependency added: a package called “peacenotwar”
- **For most users, peacenotwar leaves a manifesto on their desktop**
- **If the user’s IP address is in Russia or Belarus, another payload activates**
  - Under one variant, any file the script can access is overwritten with a ‘ ’ emoji, causing widespread data loss
- **Impacted a large number of Node.js programs**
  - Any that depended on affected versions of node-ipc



https://www.bleepingcomputer.com/news/security/big-sabotage-famous-npm-package-deletes-files-to-protest-ukraine-war/

Shai-Hulud: automating supply-chain attacks

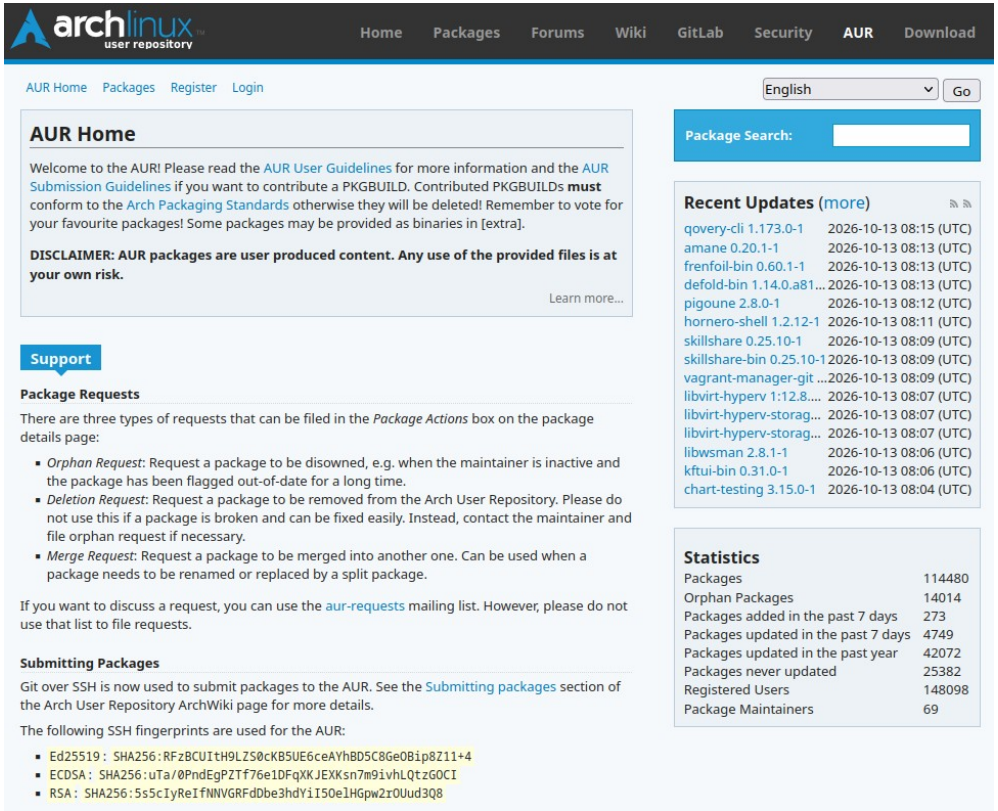
- **Self-replicating worm: steals credentials (tokens) of developers who install it**
  - Then poses as them to insert malware into published packages
- **Initial Sep. 2025 version infected 500+ packages**
- **To hamper spread, npm is rolling out new authentication requirements**
  - Prohibit publishing solely through an easily-stolen auth token
- **New worm variant still active as of October 8**



John Schoenherr cover art for *Analog*
https://dune.fandom.com/wiki/Shai-Hulud

Arch User Repository

- **Community-supported repository of Arch Linux packages**
  - Unverified, like npm: malicious packages do show up
- **June 2026: Attackers exploit method to take over abandoned (orphan) packages**
- **Malware inserted into 1,900+ packages automatically**
  - Downloads and runs malicious binary from npm
  - Infostealer malware harvests credentials of users
- **Users are expected to read and audit AUR packages themselves when installing**
  - However, mistakes happen, and attackers count on this



https://aur.archlinux.org/

OpenSSH

- **Open Secure Shell**
  - Allows connecting a terminal to a computer over the Internet
- **SSH protocol encrypts the connection**
  - Avoids an intruder seeing what commands are being sent, or making malicious modifications
- **Part of the OpenBSD project**
  - Berkeley Standard Distribution
  - A Unix-like operating system similar to Linux
- **Critical piece of security infrastructure**
  - Some SSH servers are exposed directly to the Internet
- **OpenSSH server runs as root user**
  - Hijacking OpenSSH would allow complete server takeover



https://www.openssh.org/

Disaster strikes

https://www.openwall.com/lists/oss-security/2024/03/29/4
Date: Fri, 29 Mar 2024 08:51:26 -0700
From: Andres Freund <andres@...razel.de>
To: oss-security@...ts.openwall.com
Subject: backdoor in upstream xz/liblzma leading to ssh server compromise

Hi,

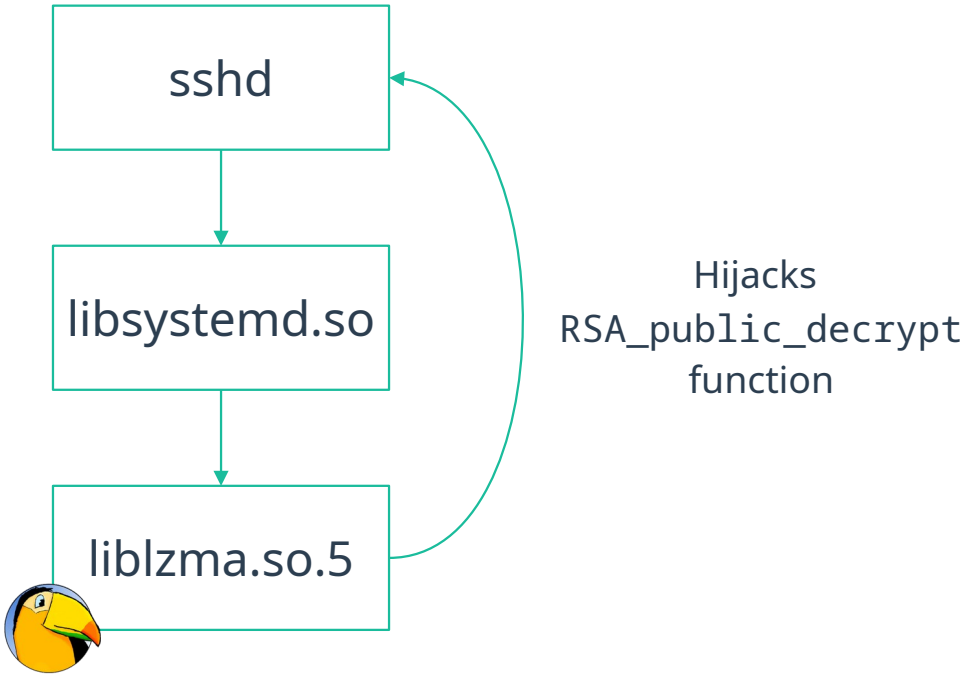
After observing a few odd symptoms around liblzma (part of the xz package) on Debian sid installations over the last weeks (logins with ssh taking a lot of CPU, valgrind errors) I figured out the answer:

The upstream xz repository and the xz tarballs have been backdoored.

At first I thought this was a compromise of debian's package, but it turns out to be upstream.

XZ Utils backdoor incident

- **April 2024: A Microsoft developer discovers an anomaly**
- **An RSA decryption routine in OpenSSH was hijacked to call a function in liblzma, part of XZ Utils**
  - Disrupts normal authentication process
  - An attacker with the right key can run any command as the root user
- **How did liblzma hijack OpenSSH?**
  - Linux distributions added patches to integrate with systemd, the init system
  - Dynamically linking systemd brought in liblzma and its backdoored RSA function



Social engineering: how XZ was compromised

- **xz-utils compromised through social engineering attack**
- **Lead developer Lasse Collin pressured to add additional maintainers**
  - Users he interacted with on mailing lists are suspected to be sockpuppets
- **Threat actor going by "Jia Tan" alias begins contributing to the project**
  - Over a span of two years, Jia Tan builds reputation
  - Gains substantial control over the project, and even its website
- **The xz-utils project, and Lasse Collin, were identified as a weak link**
  - Ultimately, his trust was exploited
- **Pressure put on distribution maintainers to quickly release (secretly backdoored) versions**

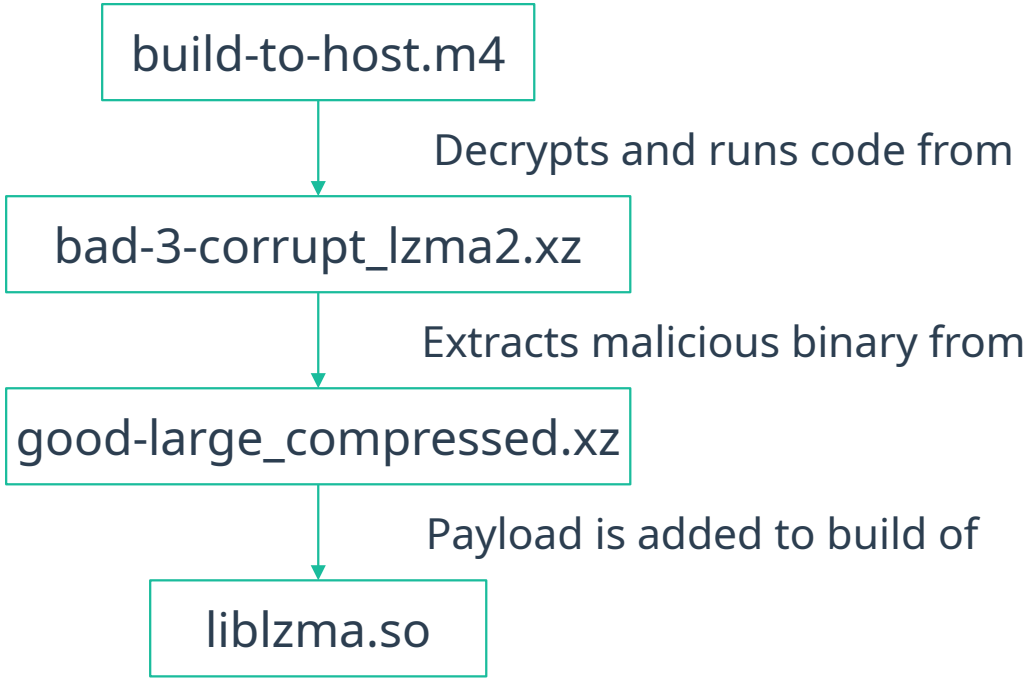
Jigar Kumar, 2022-06-07
https://www.mail-archive.com/xz-devel@tukaani.org/msg00566.html

Progress will not happen until there is new maintainer. XZ for C has sparse commit log too. Dennis you are better off waiting until new maintainer happens or fork yourself. Submitting patches here has no purpose these days. The current maintainer lost interest or doesn't care to maintain anymore. It is sad to see for a repo like this.

> **Lasse Collin**, 2022-06-08
> https://www.mail-archive.com/xz-devel@tukaani.org/msg00567.html
>
> I haven't lost interest but my ability to care has been fairly limited mostly due to longterm mental health issues but also due to some other things. Recently I've worked off-list a bit with Jia Tan on XZ Utils and perhaps he will have a bigger role in the future, we'll see.

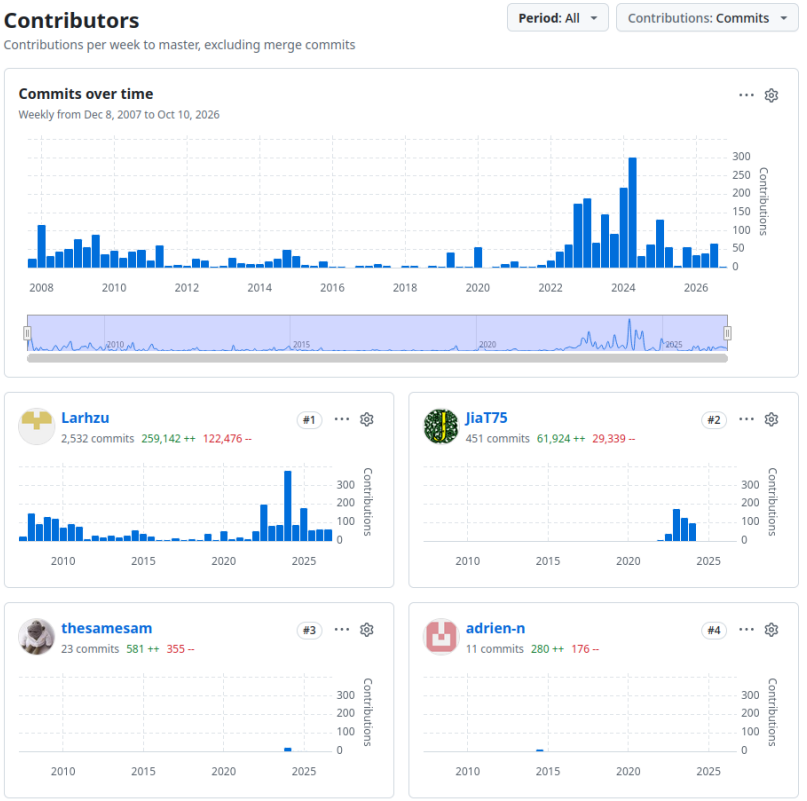
Stealth

- **No source code for the backdoor was ever committed to GitHub**
  - Multistage setup hidden in supposed (unused) test files
  - Disguised as .xz archives
- **Build process decrypts test file into a binary blob**
  - Linked with liblzma during the build
- **Some users noticed errors when running xz within Valgrind**
  - Jia Tan quickly added a patch to avoid this error triggering suspicion
- **The backdoor was a carefully-concealed weapon**
  - Was incorporated into multiple distributions, but discovered in time to avert the worst outcome



Where are we today?

- **After the backdoor was uncovered, Jia Tan vanished**
- **Lasse Collin still responsible for the vast majority of work on XZ Utils**
  - Nobody other than Collin has surpassed Jia Tan in number of contributions
- **Linux distributions have substantially cut down on dynamic links within OpenSSH and systemd**
  - No longer linked to sshd (at least on Debian)
- **The underlying social vulnerability still remains**
  - The xz-utils backdoor was found: what have we *not* discovered?



https://github.com/tukaani-project/xz/graphs/contributors

Acknowledgements

- With thanks to former Hashdump Financial Officer Eli Povolny, who presented this topic two years ago
- Cover image: “Toucan Parque-das-Aves” by Acediscovery, licensed under Creative Commons Attribution 4.0 International https://commons.wikimedia.org/wiki/File:Toucan_Parque-das-Aves.jpg

References (1/2)

- Chris Prall. "What Is a Supply Chain Attack? Types, Examples, and Prevention." Aug. 31, 2026. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/supply-chain-attack/
- Dina Temple-Raston. "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack." Apr. 16, 2021. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
- Ax Sharma. "BIG sabotage: Famous npm package deletes files to protest Ukraine war." Mar. 17, 2022. https://www.bleepingcomputer.com/news/security/big-sabotage-famous-npm-package-deletes-files-to-protest-ukraine-war/
- Tyler Resch. "RIAEvangelist/node-ipc is malware / protest-ware." Mar. 16, 2022. https://gist.github.com/MidSpike/f7ae3457420af78a54b38a31cc0c809c
- Aviad Gershon. "Protestware, Politics, and Open-Source Software." Mar. 17, 2022. https://checkmarx.com/blog/protestware-politics-and-open-source-software/
- Microsoft Defender Security Research Team. "Shai-Hulud 2.0: Guidance for detecting, investigating, and defending against the supply chain attack." Dec. 9, 2025. https://www.microsoft.com/en-us/security/blog/2025/12/09/shai-hulud-2-0-guidance-for-detecting-investigating-and-defending-against-the-supply-chain-attack/
- Brandon Vigliarolo. "Shai-Hulud worm makes jump to AI infrastructure with Tensorlake compromise." Oct. 8, 2026. https://www.theregister.com/security/2026/10/08/shai-hulud-worm-makes-jump-to-ai-infrastructure-with-tensorlake-compromise/5302054

References (2/2)

- Cybersecurity & Infrastructure Security Agency. "Widespread Supply Chain Compromise Impacting npm Ecosystem." Sep. 23, 2025. https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem
- lenucksi. "AUR Malware Check — June 2026 Campaign & Cross-Campaign Detection." Jun. 24, 2026. https://github.com/lenucksi/aur-malware-check/blob/master/data/campaigns/aur-infected/packages.txt
- Andres Freund. "backdoor in upstream xz/liblzma leading to ssh server compromise." Mar. 29, 2024. https://www.openwall.com/lists/oss-security/2024/03/29/4
- Akamai Security Intelligence Group. "XZ Utils Backdoor — Everything You Need to Know, and What You Can Do." Apr. 1, 2024. https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know
- Dan Goodin. "What we know about the xz Utils backdoor that almost infected the world." Apr 1, 2024. https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/
- Mario Lins et al. "On the critical path to implant backdoors and the effectiveness of potential mitigation techniques: Early learnings from XZ." Apr 13, 2024. https://arxiv.org/abs/2404.08987v1
- Sam James. "FAQ on the xz-utils backdoor (CVE-2024-3094)." Updated Jan. 26, 2025. https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27
- Anthony Weems. “xzbot.” Apr. 1, 2024. https://github.com/amlweems/xzbot


Questions?