Italian Linux Society

FOSS, XZ, NSA

ed altre lettere (piuomeno) a caso

Italian Linux Society?

- Dal **1994**, **Linux** in **Italia**
- Dal **2001** il **Linux Day**, la principale manifestazione italiana dedicata al **software libero**, la **cultura aperta** e la **condivisione**!

Lettere a caso?

- FOSS
- NSA
- XZ & LZMA
- CVE & CVSS
- Compro una vocale

FOSS

Free and **Open Source Software**

Secondo la Free Software Foundation un software si può definire

libero

solo se garantisce quattro

libertà fondamentali

FOSS (0)

Libertà di **eseguire il programma**

- per qualsiasi scopo.
- per/da qualsiasi persona od organizzazione
- su qualsiasi tipo di sistema informatico
- per qualsiasi tipo di attività

FOSS (1)

Libertà di

- **Studiare**
  - come funziona il programma
- **Modificare**
  - il programma in base alle proprie necessità

FOSS (2)

Libertà di **Ridistribuire**

copie del programma

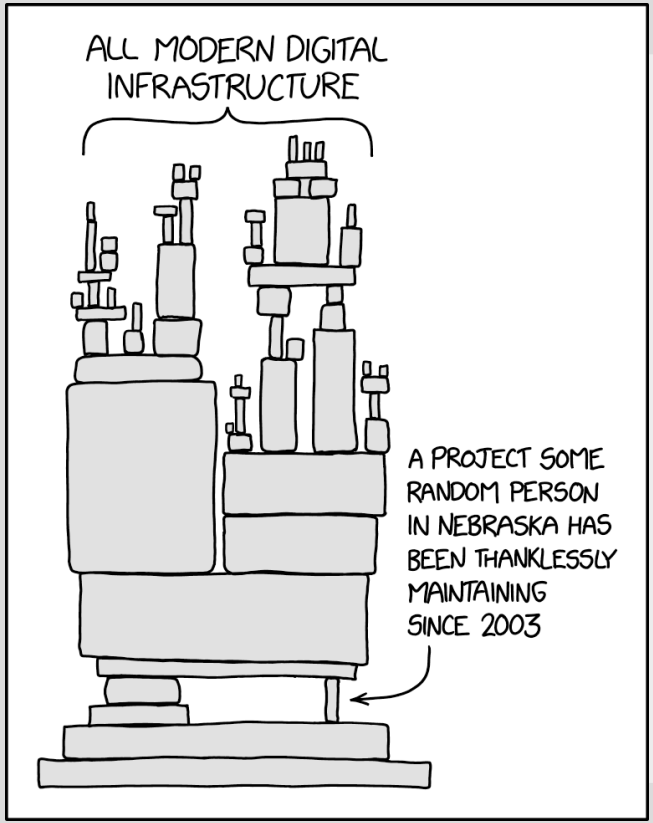
in modo da aiutare il prossimo

FOSS (3)

Migliorare il programma

- **distribuire pubblicamente** i miglioramenti *in modo tale che tutta la comunità ne tragga beneficio.*
- questa libertà comprende quella di **usare** e **rilasciare le versioni modificate** come software libero.

FOSS (?)



Cosa c'entra
con Cybersecurity
Software Libero
e Nebraska?

FOSS => XZ

- XZ Utils e libLZMA sono progetti Open Source
  - In particolare **pubblico dominio/GPL**
- Vengono utilizzate per implementare l'algoritmo di compressione LZMA
- Utilizzato per le connessioni remote SSH

XZ (1) => CVE/CVSS (?)

Altre lettere a caso: **CVE** e **CVSS**

- CVE-2024-3094 – CVSS 10.0 (record!)
- **Common Vulnerabilities** and **Exposures** è un **dizionario di vulnerabilità** e falle di sicurezza note pubblicamente.
- **Common Vulnerability Scoring System**...

...ma ci interessa?

XZ (2) => Ingegneria Sociale

No!

A noi oggi interessa la **backstory**!

- https://robmensching.com/blog/posts/2024/03/30/a-microcosm-of-the-interactions-in-open-source-projects/
- https://www.mail-archive.com/xz-devel@tukaani.org/msg00562.html
- https://robmensching.com/blog/posts/2024/03/31/what-could-be-done-to-support-open-source-maintainers/

XZ (3)

Step 0:

- Il mantainer è esausto (*burns out*), non ha tempo né forze adeguate per dedicarsi appieno al progetto

XZ (4)

- *“Is XZ for Java still maintained? I asked a question here a week ago and have not heard back.”* - https://www.mail-archive.com/xz-devel@tukaani.org/msg00562.html
- Al **mantainer** viene chiesto se una determinata feature sia ancora **supportata** e **mantenuta**.

XZ (5)

- *“Yes, by some definition at least, like if someone reports a bug it will get fixed. Development of new features definitely isn’t very active. :-(” -* https://www.mail-archive.com/xz-devel@tukaani.org/msg00563.html
- Il mantainer inizia a sentirsi **ingiustamente** “colpevole”: non ha sbagliato nulla, eppure si sente **responsabile**

XZ (6)

- *“Jia Tan has helped me … and he might have a bigger role in the future … It’s clear that my resources are too limited … so something has to change in the long term.”* - https://www.mail-archive.com/xz-devel@tukaani.org/msg00563.html
- Nella stessa risposta introduce chi in questi anni lo ha *aiutato*, annunciando che in un futuro prossimo potrebbe avere un **ruolo più rilevante** nel progetto.

XZ (7)

- ***“Progress will not happen until there is new maintainer. … The current maintainer lost interest or doesn’t care to maintain anymore. It is sad to see for a repo like this.” -***
  https://www.mail-archive.com/xz-devel@tukaani.org/msg00566.html
- Il primo attacco da parte di qualcuno che sembra *esterno* alla faccenda

XZ (8)

- *“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.” - “It’s also good to keep in mind that this is an **unpaid hobby project**”* https://www.mail-archive.com/xz-devel@tukaani.org/msg00567.html
- Il mantainer prova a difendersi dalle accuse, dovendo sottolineare l’ovvio: è un progetto di **pubblico dominio** (neanche GPL!), eppure se può contribuisce.

XZ (9)

- *“You ignore the many patches bit rotting away on this mailing list.* ***Right now you choke your repo. Why wait until 5.4.0 to change maintainer? Why delay what your repo needs?” -***
  https://www.mail-archive.com/xz-devel@tukaani.org/msg00568.html
- Gli attacchi continuano, suggerendo di **accelerare il passaggio di consegne** già anticipato dallo stesso mantainer in precedenza.

XZ (10)

- *"**Why not pass on maintainership for XZ for C** so you can give XZ for Java more attention? Or pass on XZ for Java to someone else to focus on XZ for C? **Trying to maintain both means that neither are maintained well.**" -* https://www.mail-archive.com/xz-devel@tukaani.org/msg00569.html
- Anche un *apparentemente altro* sviluppatore supporta la linea suggerita.

XZ (11)

- *“Jia Tan may have a bigger role in the project in the future. He has been helping a lot off-list and is practically a co-maintainer already. **:-)**”* - https://www.mail-archive.com/xz-devel@tukaani.org/msg00571.html
- Il danno è fatto, suggellato dalla faccina.
- **Lo scambio di mail si chiude qui.**

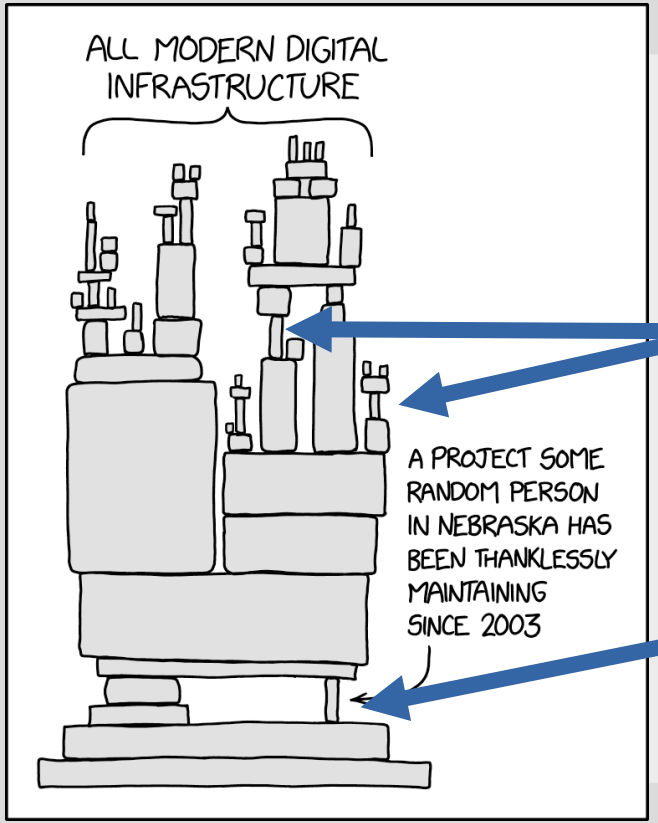
XZ (12)

- Questa conversazione avviene tra il **19 Maggio** ed il **29 Giugno 2022**.
- La versione compromessa viene annunciata dallo stesso “Jia Tan” il **24 Febbraio 2024.**
- **Si ripete con la patch successiva il 9 Marzo.**

XZ (13)

Verrà scoperto da **Andres Freund** soltanto il **29 Marzo**, notando **600 millisecondi** di ritardo ed un **insolito carico** sulla CPU.

FOSS (!)



Altre librerie e progetti

XZ

Altri Notabili Esempi

NSA ha regalato SELinux, un modulo di sicurezza, al progetto Linux.

Non sono presenti falle, *se utilizzato correttamente.*

NSA (1)

Eppure, si sospetta che NSA abbia provato almeno tre volte ad inserire delle backdoor in Linux e progetti correlati:

- Bitkeeper
- PRNG di OpenSSL
- Bvp47

NSA (2)

Chi le ha scoperte?

È famoso oggi?

Tre al prezzo di uno

- ANoM (ΛNØM)
- FBI
- AFP

FBI && AFP (1)

ANOM, un cellulare che prometteva completo anonimato e sicurezza.

...turns out it was a honeypot.

Okay, basta

La lista di **backdoor** riguardanti **Software Libero è infinita**. Alcune sono state scoperte subito, altre dopo anni o solo dopo gli avvisi di garanzia.

Cosa possiamo fare noi?

A New Hope

Non è colpa del Software Libero.

- Cosa ci insegna XZ? L'attacco **non** è stato informatico, ma **sociale**.
- Se al mantainer fosse stato offerto un lavoro a tempo pieno su XZ Utils? Se gli fossero stati offerti soldi? Se fosse stato minacciato?
  Il risultato sarebbe stato lo stesso.

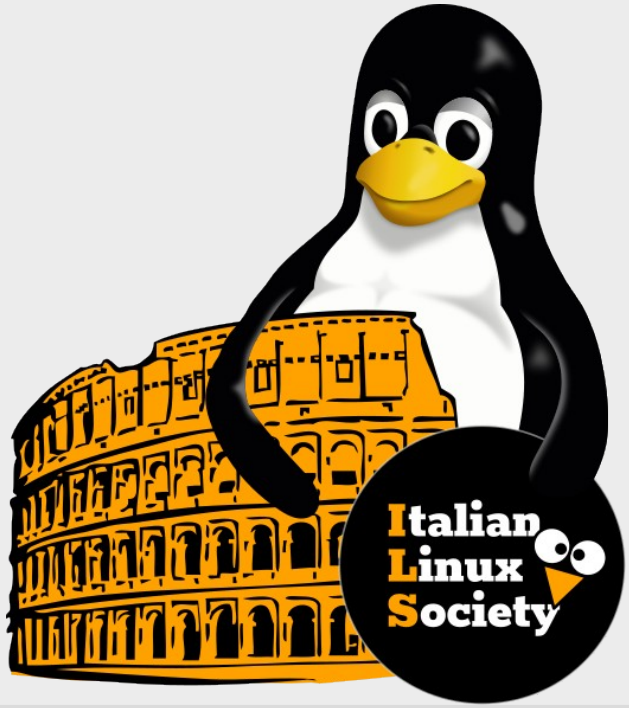
The Empire (always) Strikes Back

Le quattro libertà del Software Libero
sono un **garante**,
ma serve il **supporto della comunità.**

Domande?

"Perché dovrei sviluppare o supportare il Software Libero?"

Goodbye, and thanks for all the fish!



io sono
tucs@linux.it

KTHXBYE