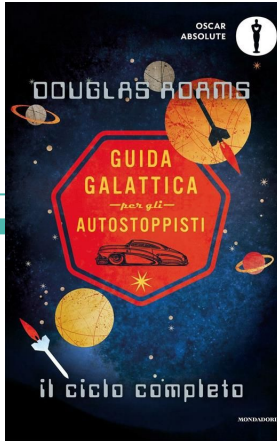
DON’T PANIC *

Lavoro c’è la fuori *



log4j

Un'innocua **libreria** di logging per Java

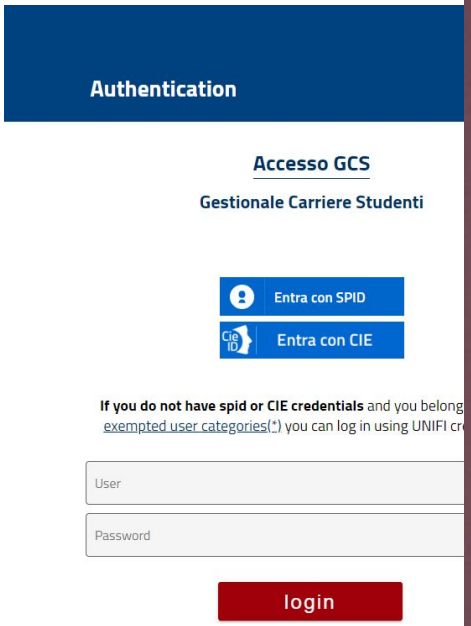
9 Dicembre 2021

Falla di sicurezza grave (CVE-2021-44228)

=

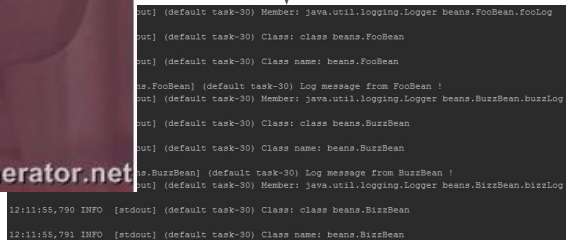
PANICO

Login flow

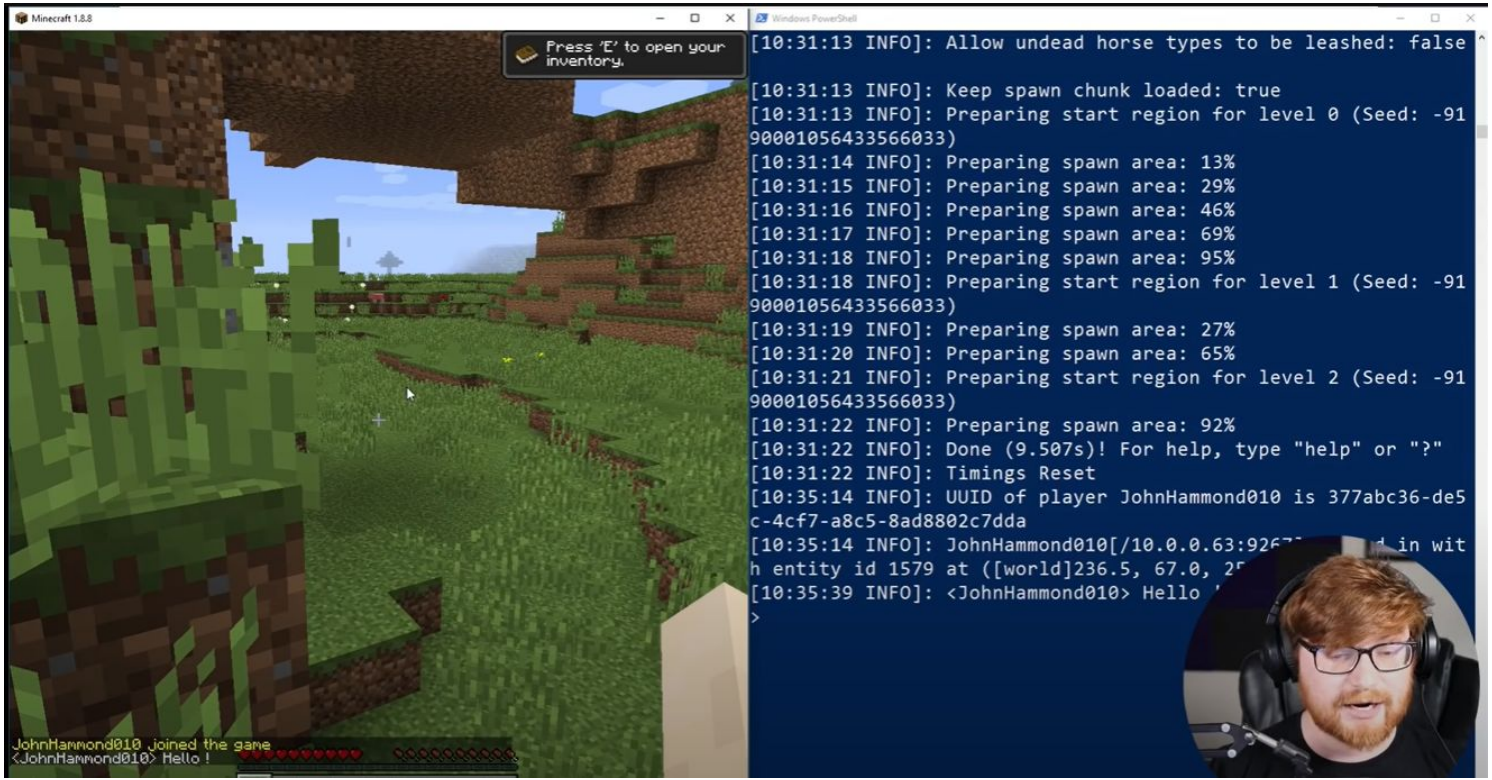


Java

Log

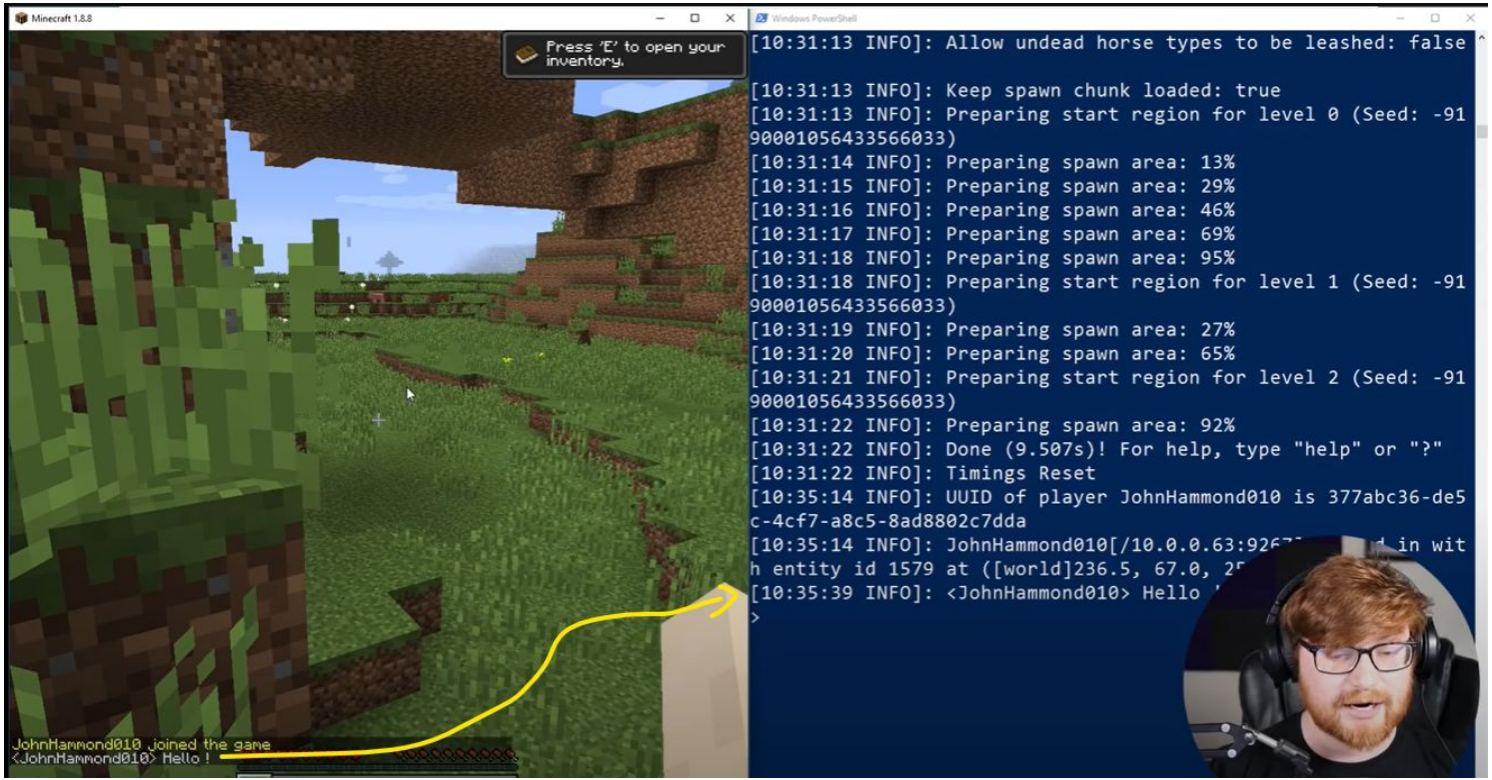


?



https://www.youtube.com/watch?v=7qoPDq41xhQ

Minecraft injection point

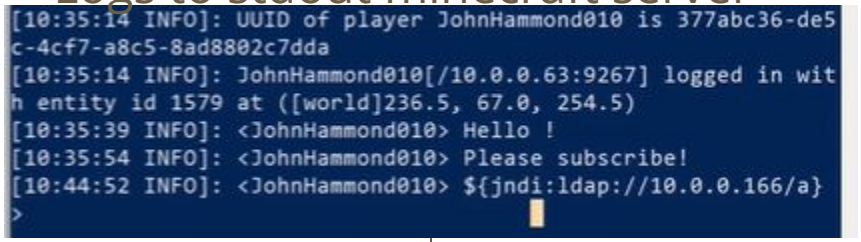


https://www.youtube.com/watch?v=7qoPDq41xhQ

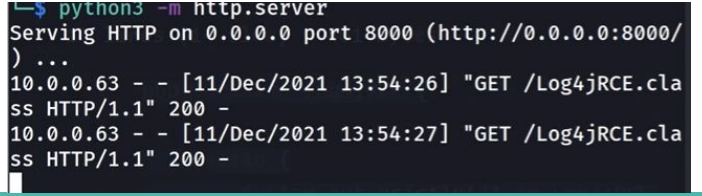
Log4shell attack

Chat

Logs to stdout minecraft server



Hacker server listening on 10.0.0.166



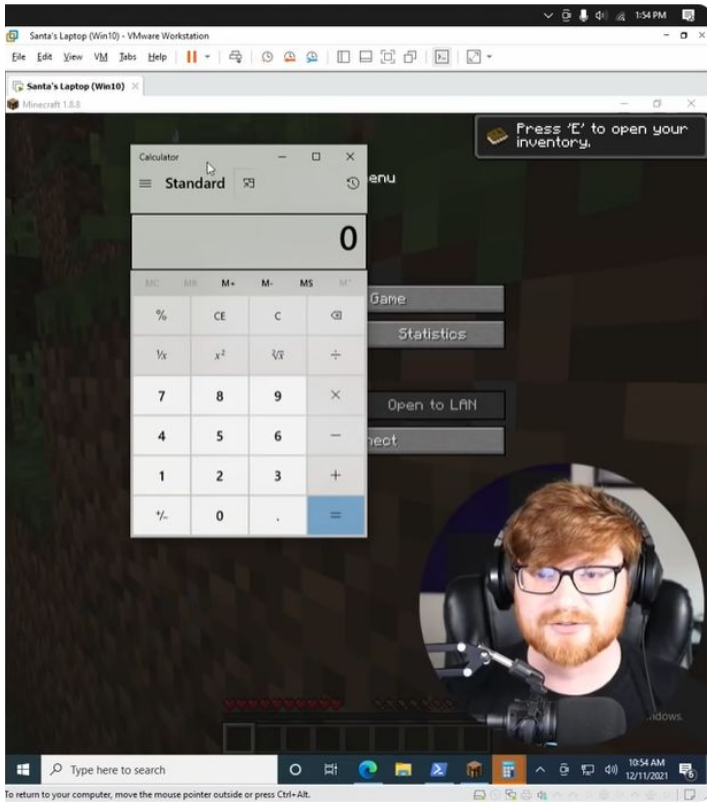
“Malicious” code to inject

File Edit Search View Document Help

```
1 public class Log4jRCE {
2
3     static {
4
5         try {
6             Runtime.getRuntime().exec("calc.exe").waitFor();
7         } catch (Exception e) {
8             e.printStackTrace();
9         }
10    }
11
12 }
```

https://www.youtube.com/watch?v=7qoPDq41xhQ

Result



https://www.youtube.com/watch?v=7qoPDq41xhQ

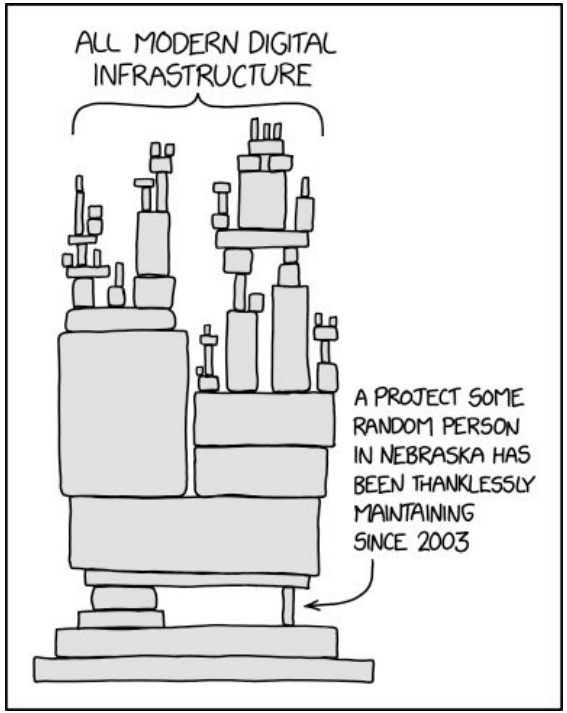
Timeline

- **18 luglio 2013**: Apache rilascia Log4J 2.0-beta9 – da questo momento in poi **nasce Log4Shell**
- **9 dicembre 2021** vulnerabilità pubblica
- **28 dicembre 2021** final patch
- **4 gennaio 2022** Federal Trade Commission (FTC) degli Stati Uniti intende perseguire le aziende vulnerabili a causa di Log4Shell
- **Maggio 2023**: Log4Shell è ancora la seconda vulnerabilità più comunemente sfruttata (“Check Point” report)

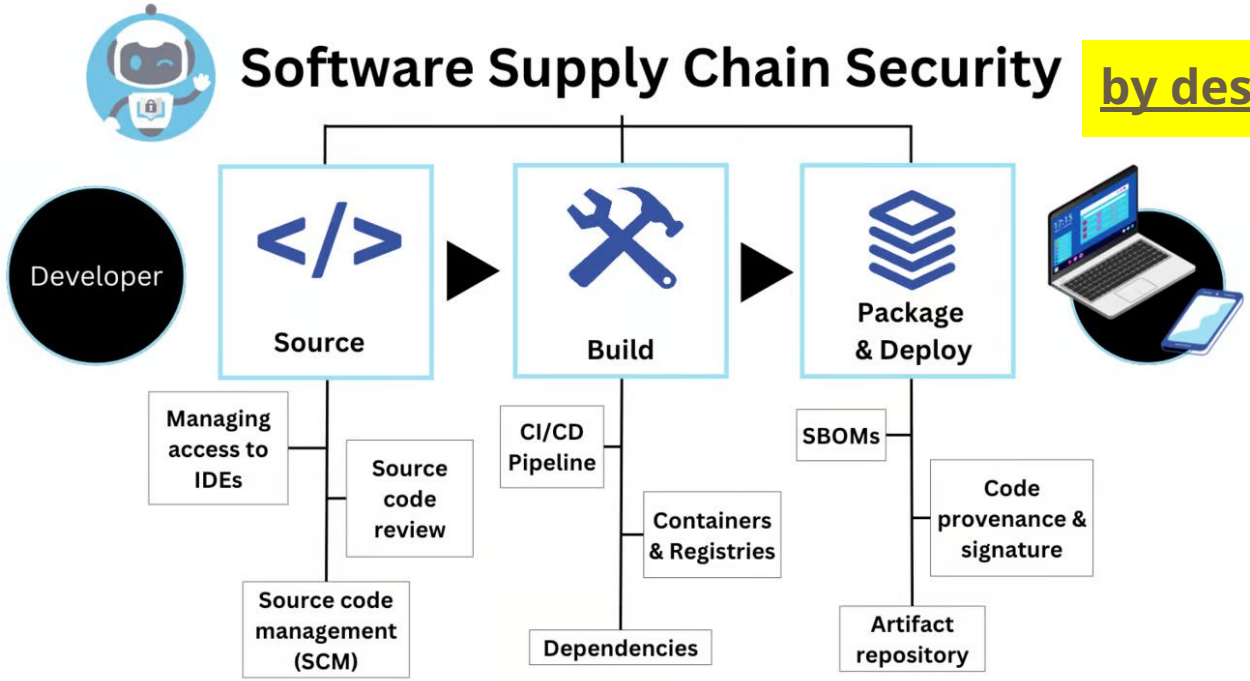
https://www.ibm.com/it-it/topics/log4j

Software supply chain

“s**t happens” → farsi trovare pronti



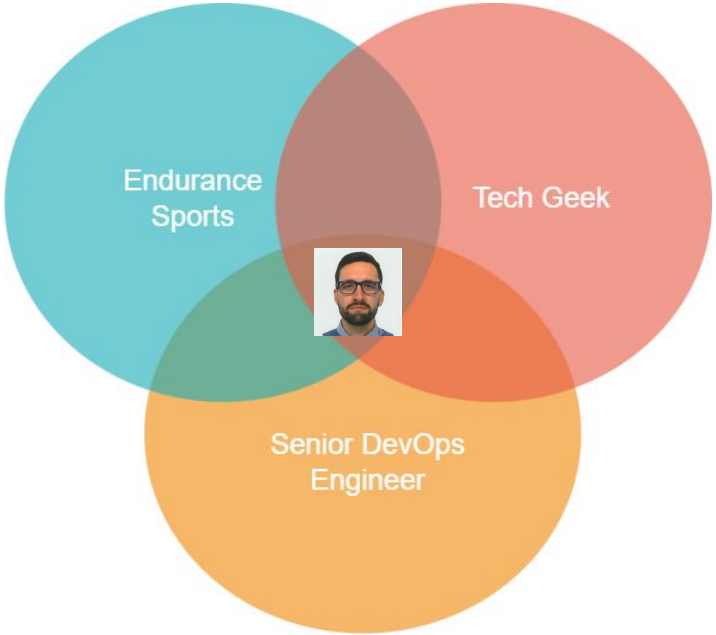
Software supply chain



https://tldrsec.com/p/supply-chain-security-overview

Chi sono / cosa faccio

yuribacciarini.com



(My) 3 TIPS

1) Postura di **apprendimento** continuo

2) **Testarsi**

Aziende

- prodotto
- servizi
- servizi cybersecurity
- consulenza
- start-up
- web agency

(My) 3 TIPS

3) Inglese

Quante persone parlano Italiano?
85 Milioni (1%)

.. e inglese?
1,5 Miliardi (18%)

+1

4) Mettere in discussione tutto “continuamente”

*"Nel mondo della **cybersicurezza**, un **ingegnere di database** che scopre inavvertitamente una **backdoor** in una funzione fondamentale di **Linux** è un po' come un **panettiere** che sente l'odore di una pagnotta appena sfornata, intuisce che qualcosa non va e deduce correttamente che qualcuno ha manomesso l'intera fornitura globale di lievito. È il tipo di intuizione che richiede anni di esperienza e **un'attenzione ossessiva ai dettagli**, oltre a una sana dose di fortuna -*
K. Roose, NYT"

Q&A