Red Hat

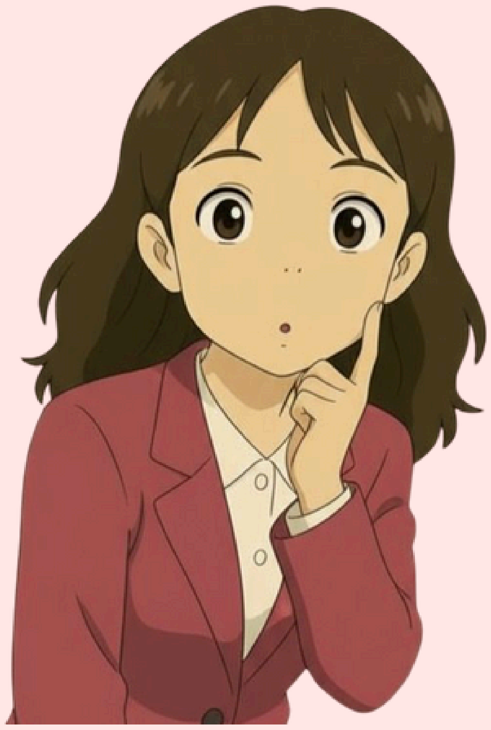
Got Hacked

What Actually Happened?

Nensi Ravaliya

My First Reaction

Wait, Red Hat? **THE Red Hat?**



Red Hat

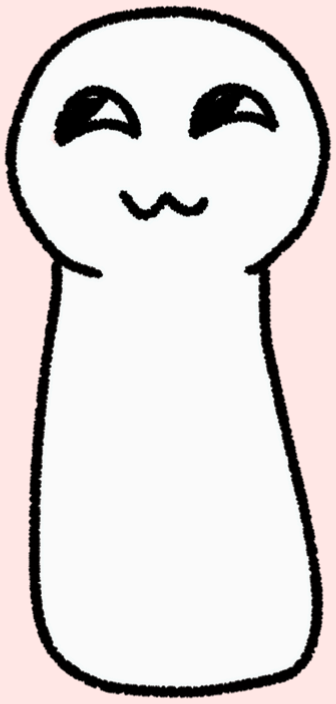
- The **open-source security giant** with entire teams dedicated to protecting systems.
- Yep. They got breached and that’s exactly what makes it scary.

What Actually Happened

A hacker group, **Crimson Collective**: broke into Red Hat's internal GitLab.

➤ Stole **570GB of data**
➤ From **28,000 repositories**
➤ Impacted **800+ organizations**
Including **IBM, Siemens, Verizon**… even the **NSA**.

-> What They Stole



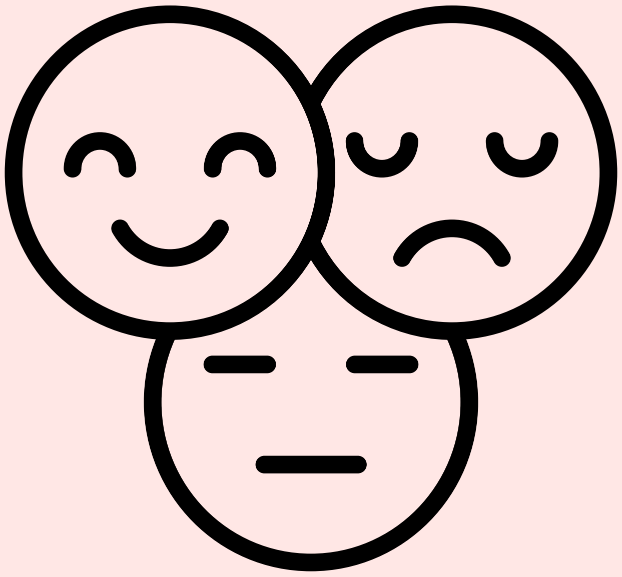
Not random file but the **blueprints of companies.**

- **Network diagrams**
- **Database passwords**
- **Access tokens & API keys**
- **VPN configurations**
- **Architecture details**

Basically -> everything a hacker dreams of.

→

-> Who Got Hit



The list is heavy:

- **Banks** -> JPMorgan, HSBC, Citi
- **Tech** -> IBM, Cisco, Adobe, Siemens
- **Telecom** -> Verizon, AT&T, T-Mobile
- **Government** -> NSA, DoD, U.S. Senate
- **Healthcare** -> Mayo Clinic, Kaiser Permanente

If your org used Red Hat Consulting…
it's time to check.

→

Nensi Ravaliya

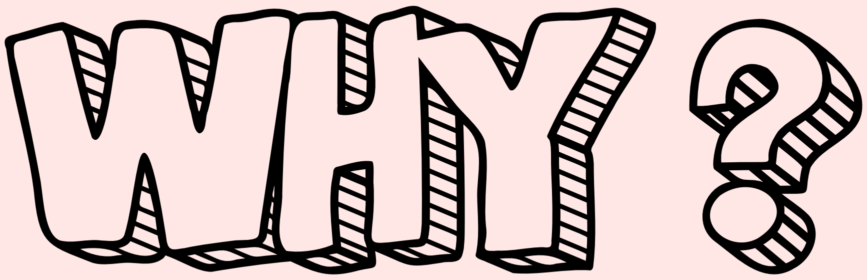
How They Got In

Just human mistakes.

- **Found leaked credentials online**
- Logged into Red Hat’s GitLab
- **C**reated new admin accounts
- Downloaded everything (**570GB**)
- Vanished. Then demanded payment.

They didn’t even need zero-days, just passwords.

Why This Matters



- If Red Hat can get hacked, so can we.
- Not fear-mongering. Just facts.
- Security teams, budgets, tools, all failed because...

👉 **Someone left old credentials lying around.**

The Real Danger

DANGER

▲ Hackers might already be using those stolen credentials

▲ **Consulting environments = goldmines for attackers**

▲ 5 years of exposure (**2020–2025 data**)

That means old projects, same keys, still active.

What You Should Do Right Now

1. **Rotate all credentials** (passwords, API keys, tokens)
2. **Check logs** since Sept 2025 for strange access
3. **Audit what Red Hat had access to**
4. **Scan repos** for exposed secrets
5. **Enable advanced monitoring**
6. **Brief your teams:** Security, Legal, Management
7. **Do it now, not later**.

The Uncomfortable Truth

Red Hat had:

- World-class security teams
- Unlimited budgets
- Years of expertise

But consulting environments are different.

- They’re built for access, not isolation.
- And that’s what made them vulnerable.

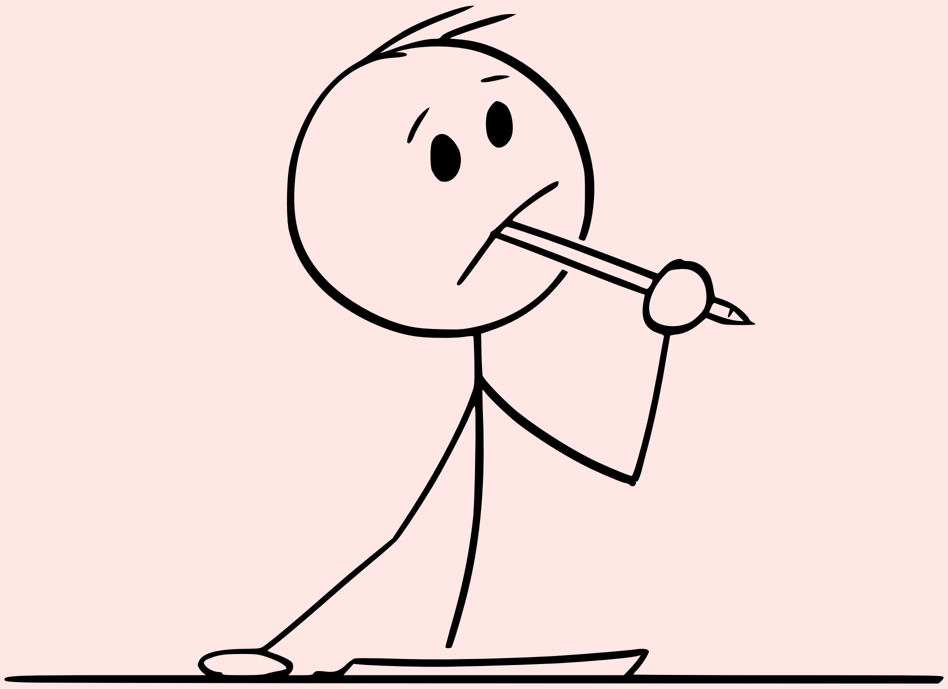
The Lesson

Security isn’t luck. It’s discipline.

LESSON

◆ Rotate credentials regularly
◆ Actually read your security logs
◆ Protect Dev/Consulting environments like production
◆ Assume exposure always
◆ Have a response plan ready

Final Thought



Red Hat says their products (**RHEL, OpenShift**) are safe.

But if the consulting GitLab had weak spots…
What else might?

This breach is more than a headline, it's a mirror for every organization.

Nensi Ravaliya

-> Remember

Security isn’t about “**if**.”
It’s about “**when**.”

- Stay alert.
- Stay prepared.
- **Stay humble -> even giants fall.**

Repost and Follow

Nensi Ravaliya

for more content

Want to build your career in cloud?

Subscribe to Yatri Cloud Channel