9r13f

or

A botnet pwned our production servers

DevOops Amsterdam #7 - 17 September 2024

A botnet pwned our production servers

- 7h3 3v3nt
- 7h3 5ve phas3s 0f 9r13f
- Moving forward

7h3 3v3nt

7h3 53tup

- 14 January 2014
- Working on SourceLair; an online IDE for web development
- Tens of thousands of users in production

7h3 3v3nt

- We SSH into the server and notice a few things
- Some binaries (e.g. `ls`) have been `touch`ed
- Some of our users’ private keys have been deleted
- A l33t named file has appeared pointing out we got PWNED

7h3 5ve phas3s 0f 9r13f

Phase I: Denial

Denial

- It can’t be real
- Maybe someone from the team made a joke
- Let me check again

Phase II: Anger

Anger

- Why would anyone create malicious software?
- Why would not Rackspace use stronger default passwords?
- Why no one thought about this potential threat?

Phase III: Depression

Depression

- I guess we do not deserve the trust of our users
- Chances are good I am the stupidest person in the world
- At least it was a nice ride

Phase IV: Bargaining

Bargaining

- OK, what now?
- How should we handle this?
- What can we publish without damaging our reputation?

Phase V: Acceptance

Acceptance

- The past cannot change
- Come absolutely clean about the incident
- Take actions for the future

Post mortem time! 🥲

14 Jan 2014 security breach post-mortem

Root access gained by botnet. No data steal or corruption has been verified.

On Tuesday, 14th of January 2014, the main application server of sourceLair got hacked, and the intruder gained root access on it. The security breach was result of the lack of suspiciousness of the engineering team of sourceLair. As it seems to be, the intruder was a botnet, not a human, and no data was stolen or got corrupted. Despite that, security measures had to be taken from the engineering team, and more security measures will have to be taken by both the engineering team and the users themselves to ensure 100% security of their personal data.

Post mortem article still alive

https://www.sourcelair.com/blog/articles/13/post-mortem-2014-01-17/

Moving forward


Ten years later...

Bare metal or cloud?

Bare metal or cloud?

- It does not matter
- We have done a full circle, from cloud to serverless and back to bare metal
- What matters is making conscious and intentional choices

A few bare metal tips

- Allow SSH access **only in a private network**
- Access your servers through a **bastion server**
- Always use **SSH key forwarding** (do not store private keys on servers)
- Allow SSH access **only via SSH key** (no password for SSH)
- Set up email notifications for SSH access

Wrapping up

Wrapping up

- **Truth** is the only way
- **Accountability** is the best option
- **Clarity** is the best foundation

whoami

- Paris Kasidiaris
- Co-founder with **LOGIC**

LOGIC

- We provide DevOps consulting services
- Learn more at https://withlogic.co
- Get in touch at hey@withlogic.co

pulses.dev