Security Concerns in Mining

Cryptocurrency miners **face countless threats** every moment...

Compromised mining pools resulting in **theft of earnings**.

Social engineering attacks on employees and service providers.

Untrustworthy

partners, employees,

and consultants.

DDoS attacks on exposed nodes and network services.

BGP hijackings routing miners to malicious pool servers.

Man-in-the-Middle attacks

between miners and mining pools.

Unencrypted mining protocols offer **zero protection** against malicious actors.

Stratum was designed for thin clients, then **repurposed for mining**.

There’s no formal specification and numerous **buggy implementations.**

At the end of the day, efforts to mitigate flaws are **no more than hacks**.

Mining rigs have
more in common with kitchen
appliances than servers.

They suffer from the **same issues as routers** and consumer IoT devices.

Everything runs as **root**.

Software rarely, if ever, receives updates.

Significant reverse engineering is required to make even small improvements.

It’s advantageous for miners to **keep improvements private**.

Is this a necessary

side effect of proof-of-work?

Mitigation Strategies

Effective security measures must be **more restrictive** than a typical data center environment.

Blacklist **all** outbound traffic from rigs.

Force machines to connect through an internal stratum proxy.

Operate core network services internally.

Implement centralized logging.

Set up an intrusion detection system.

FAIL2BAN

SNORT®

KISMET

OSSEC

Questions?

Email: hello@hashrabbit.com