LACEWORK

Top cloud security threats & trends 2022

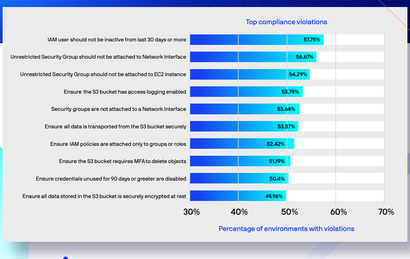
Over the past six months, Lacework Labs discovered these threats and trends in cloud security.

Cloud configuration **mistakes.**
Supply chain **vulnerabilities.**
Adapted malware that's **hard to detect.**

Cloud security posture

72% have insecure configurations

50% did not require MFA for delete operations

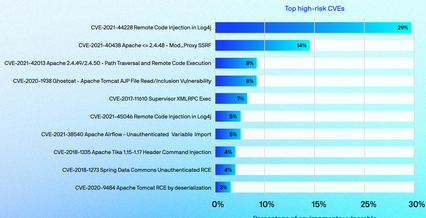


TIP: Ensure Docker APIs are not externally accessible. *Beware of malicious containers masquerading as legitimate.*

Vulnerabilities & software supply chain

<48 hrs time it takes for Muhstik to exploit remote code execution vulnerabilities

31% of malware infections use Apache Log4j



TIP: Beware! Attacks targeting third-party software libraries are on the rise. *Knowing what code you are running and where you are running it is key to responding to future incidents.*

Runtime threats & Linux malware

AV Detection Rates

74% of malicious installations on Linux workloads are dominated by a combination of XMRig, Muhstik, and Mirai

Popular Windows malware is ported to Linux with low detection rates

TIP: Implement threat intelligence focused on cloud malware and ensure *Linux support for defensive tools.*

Proactive defense & intelligence

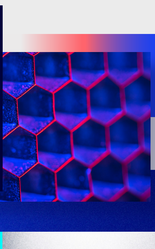
Alert defenders about post-compromise activity with canary tokens

Collect intelligence about where attackers are targeting with honeypots for improved detection

Shine a light on cloud threats continuously

- Identify all assets and quickly find misconfigurations
- Uncover host and container vulnerabilities from build to runtime
- Analyze cloud user and entity behavior for abnormalities and potential compromise

Read the 2022 Cloud Threat Report, Volume 3



Connect with us

The Lacework Labs team continues to build and expand our online presence in an effort to contribute back to the security community. Below are areas where you can find and follow our innovative threat research. **Click here to learn more!**