```
"Sid": "VisualEditor2",
            "Effect": "Deny",
            "Action": [
                "iam:CreateAccessKey"
```

```
privelege escalation
"arn:aws:iam::078657857355:user/*admin*"
```

sysdig

TWENTY23

GLOBAL CLOUD THREAT REPORT

Attacks in the cloud are lightning-fast, with minutes determining the line between detection and severe damage.

1

Cloud Automation Weaponized

Reconnaissance alerts: attack incoming

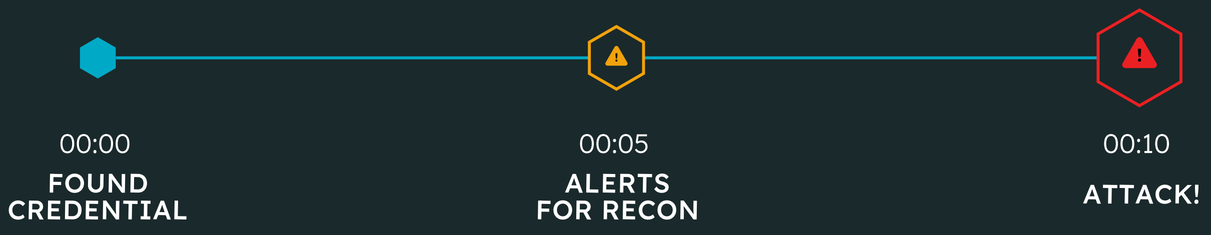
Cloud attacks happen fast. Recon and discovery are even faster. Automating these techniques allows an attacker to act immediately upon finding a gap in the target system. A recon alert is the first indication that something is awry; a discovery alert means you're too late.

2

10 Minutes to Pain

Every ~~minute~~ second counts

Cloud attackers are quick and opportunistic, spending only 10 minutes staging the attack. According to Mandiant, the median dwell time on premises is 16 days.



00:00
FOUND CREDENTIAL

00:05
ALERTS FOR RECON

00:10
ATTACK!

3

A 90% Safe Supply Chain Isn’t Safe Enough

Static analysis leaves you open to compromise

You wouldn’t drive a car with brakes that work 90% of the time. 10% of advanced supply chain threats are invisible to preventive tools. Evasive techniques enable malicious code to hide until the image is deployed. Cloud threat detection will identify bad images in runtime.

10%
Missed Completely

4

Attackers are Hiding Among the Clouds

Cloud complexity = happy hacker

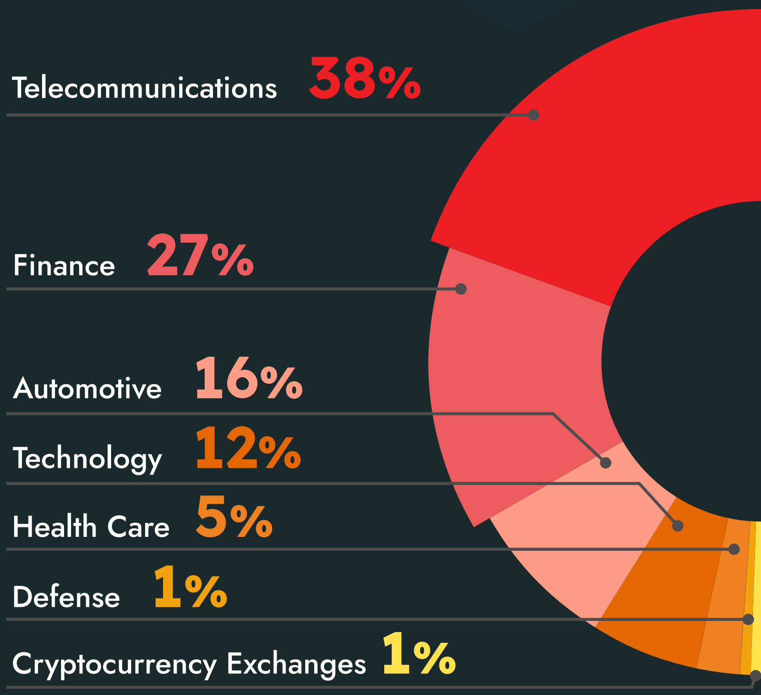
Attackers are abusing cloud services and policies to fully exploit the complexity of cloud-native environments. Using source obfuscation makes them harder to track. New techniques render IoC-based defenses ineffective, pushing blue teams toward advanced cloud threat detection.

5

65% of Cloud Attacks Target Telcos and FinTech

Attackers focus on easy cloud money

Telecommunication and finance companies are ripe with valuable information and offer an opportunity to make quick money. Cloud hackers stick to what they know — selling data like online banking info for $35 each or merchant payment accounts for $1,000+.



DOWNLOAD THE FULL REPORT

sysdig.com/2023threatreport

METHODOLOGY

The Threat Research Team at Sysdig identifies and stops the most critical cloud threats in their tracks and educates the public on the latest vulnerabilities, attack patterns, and defensive strategies for cloud environments.

This report is based on data found via open source intelligence (OSINT) and Sysdig’s global data collection — including honeypot networks — along with other publicly available information from the Falco open source community.

Sysdig conducted research in Asia, Australia, the European Union, Japan, North and South America, and the United Kingdom from October 2022 through June 2023. To stay up to date on the latest cloud threat research, trends, and best practices, visit sysdig.com/threat-research.

sysdig

EXEC-SUM-RP001 Rev. A 07/23.