When the external threats and internal risks meet - a story of cloud breach

Jay Chen, Noah McDonald

Who are we

Photo

Jay Chen

Sr. Principal Researcher

jaychen@paloaltonetworks.com

linkedin.com/in/jaychen2015

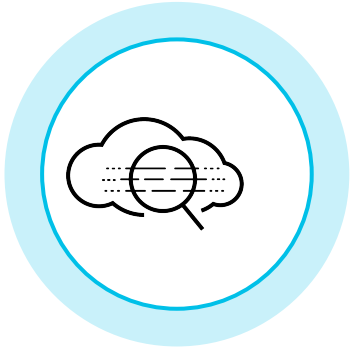
Noah McDonald

Google Cloud Consultant

noahmcdonald@google.com

https://www.linkedin.com/in/noah-mcdonald-77b04a173/

Agenda



Oversights in the Cloud

Cloud Breaches Observed

Research Data

SECTOR

We analyzed data from:

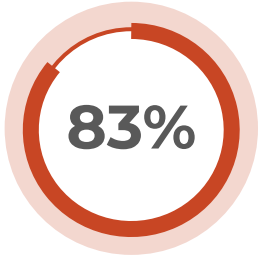
organizations

cloud environments

repositories


Oversights in the Cloud

Hard-Coded Credentials



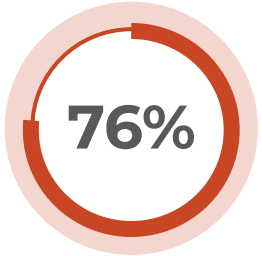
of organizations have hard-coded credentials in their source control management systems

of organizations have hard-coded credentials in virtual machines' user data

TIP

- Enable secret scanning in Source Code Management systems
- Scan secrets in Compute resources such as VMs, containers, functions

Weak Authentication



of organizations don't enforce MFA for console users

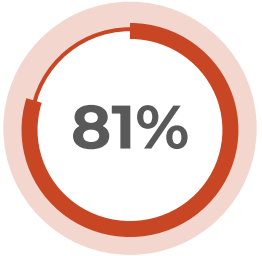
of organizations don't enforce symbols in passwords

TIP

- Enable MFA for all console logins and APIs of critical services
- Adopt federated authentication such as Okta and Active Directory

Disabled Logging

of organizations don't enforce AWS CloudTrail logging



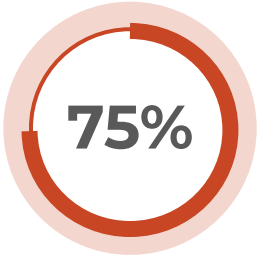
of organizations don't enforce GCP Storage bucket logging

TIP

- Always enable control plane audit logs such as AWS CloudTrail and Azure Activity Log.
- Consolidate all logs in a centralized location for easy analysis

No Automated Backup

of organizations don't enforce AWS DynamoDB point-in-time backup



of organizations don't enforce Azure Cloud SQL backup

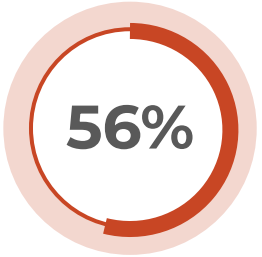
TIP

- Always automate backup processes for any cloud workload that would interrupt business operations.
- Backups should be stored in protected locations across multiple geographic locations to prevent a single point of failure

Unencrypted Data at Rest

SECTOR

of organizations don't enforce AWS EBS volume encryption



of organizations don't enforce GCP Kubernetes cluster application-layer secrets encryption

TIP

- Enable data-at-rest encryption for every cloud resource if possible
- Use customer-managed keys instead of CSP-managed keys
- Rotate encryption keys periodically

Inefficient Alert Handling

for a security alert to be resolved

of organizations take longer than four days to resolve a security alert

TIP

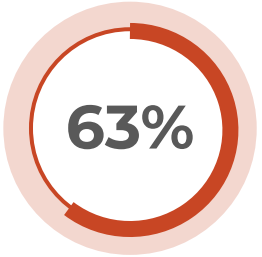
- Decrease response times by shifting security left, automated remediation and alert triage
- Identify high frequency alerts and prioritize remediation strategies

Exposed Sensitive Data

SECTOR

Sensitive data was found to exist in:

of cloud storage buckets



of publicly exposed storage buckets

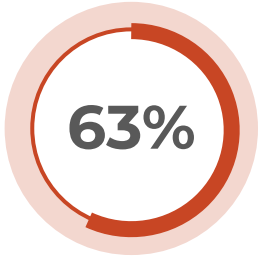
TIP

- Adopt data loss prevention (DLP) solutions to continuously identify and monitor the data with sensitive information
- Enforce policies for regulating the retention, access, and protection of sensitive information

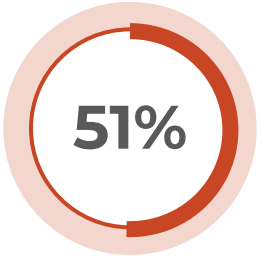
Unpatched Vulnerabilities

SECTOR

Among the source code repositories in the production:

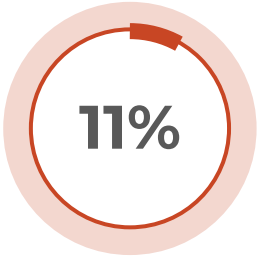


of the repositories have High or Critical vulnerabilities

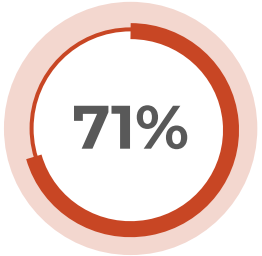


of the vulnerabilities (High or Critical) are at least two years old

Among the internet-facing services in public clouds:



of exposed hosts contain high or critical vulnerabilities



of exposed vulnerabilities (high or critical) are at least two years old

TIP

- Vulnerability scanning should be conducted in every stage of the CI/CD Pipeline
- Block code or artifacts with critical vulnerabilities from being deployed.

Impacts and Risks of Open-Source Software (OSS)

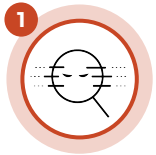
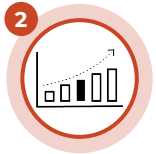
Malicious Packages in OSS

SECTOR

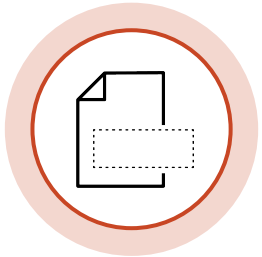
7,300

malicious OSS were identified across all major package manager registries.

Four most common techniques

1. 
   Typosquatting
2. 
   Dependency Confusion
3. 
   Account Takeover
4. 
   Self-Sabotaged OSS

Typosquatting



Typosquatting is a technique that relies on human mistakes, such as typos, when inputting a string of characters.

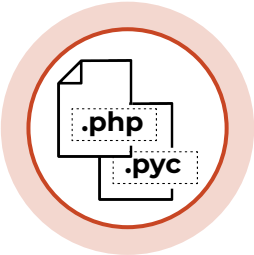
- requests is a popular Python package that many threat actors attempt to abuse.
- Packages with names such as "requessts", "requeests", "requuests", "reqquests", "reequests", and "rrequests" have been spotted in PyPi.

Dependency Confusion

Dependency confusion exploits the lack of distinction between internal and external source code repositories.

- Threat actors need to identify the packages that an organization hosts internally.
- More than **5,000** malicious packages built on this technique were discovered less than a month after the first research was published.

Account Takeover



In an account takeover attack, attackers compromise an OSS package maintainer's account and push malicious code to the legitimate repository.

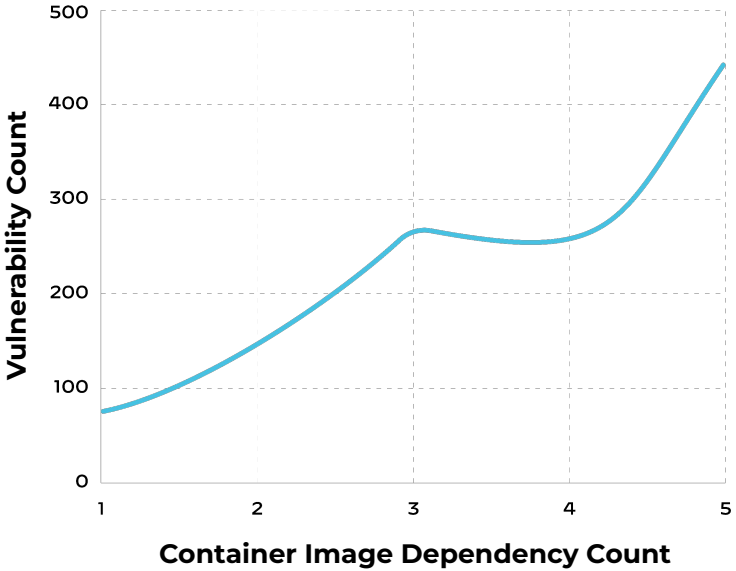
- Attackers take over an abandoned or archived repository and push malicious content to it.
- Researcher hijacked two abandoned but still popular packages, ‘Python CTX’ and ‘PHP PHPass’ to achieve an account takeover

Self-sabotage OSS

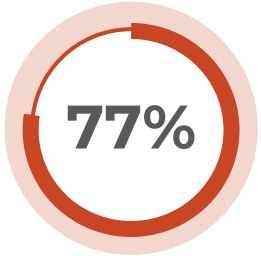
Self-sabotage happens when legitimate maintainers decide to inject malicious content into their already popular OSS projects.

- Hacktivism or revenge are often the motivations
- The author behind two popular NPM packages, ‘colors’ and ‘faker’, intentionally committed bugs into the repositories, breaking dependencies on these packages

OSS Dependency



of codebases depend on more than 100 open-source packages



of packages are non-root packages, and 77% of vulnerabilities are introduced by the non-root packages.

The number of vulnerabilities and security issues in a cloud workload is proportional to the number of external assets the workload depends on.

Cloud Breaches Observed

Common Cloud Breach TTPs

SECTOR

Initial Access
how adversary gains initial foothold within the cloud

Execution
how adversary runs malicious commands

Persistence
how adversary keeps access within compromised environment

Privilege Escalation
how adversary gains more permissions to access more resources

Exfiltration
how adversary steals data from compromised cloud workload

Impact
how adversary manipulates, interrupts, or destroys compromised cloud workloads

FROM SIM-SWAP TO DATA LEAK ON THE DARK WEB

Initial Access:

- Threat actors SIM-Swapped the engineer and took over his email and GitHub accounts
- 600 repositories were downloaded, and some source code contains cloud credentials

Persistence:

- Two backdoor users were created in the cloud account

Privilege escalation:

- The backdoor users were granted with more privileged permissions

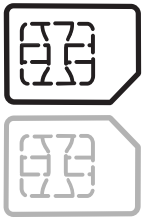
Discovery:

- Threat actors exfiltrated many database tables and storage buckets

Impact

- Threats actors left a ransom note threatening to leak data
- Some customer data were found on the dark web a few months later

Initial Access



A SIM-swap scam is a mobile phone account takeover fraud that targets two-factor authentication using SMS or phone calls.

1. An engineer lost access to GitHub
2. Trying to reset the password, they noticed they couldn't access email either
3. Trying to contact the IT, they noticed they lost cellular connectivity
4. SIM-swap attack

Persistence & Privilege Escalation


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAAAAAAAAAAAAEXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/Jack",
        "accountId": "111111111111",
        "accessKeyId": "AKIAAAAAAAAAAAAEXAMPLE",
        "userName": "Jack"
    },
    "eventTime": "2022-07-01T07:03:23Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "userName": "Jerry",
        "tags": []
    },
    "responseElements": {
        "user": {
            "path": "/",
            "userName": "Jerry",
            "userId": "AIDABBBBBBBBBBEXAMPLE ",
            "arn": "arn:aws:iam::111111111111:user/jerry",
            "createDate": "Jul 01, 2022 07:03:23 AM"
        }
    },
    "requestID": "392e2954-6ea3-9053-12b1-acff9e987d21",
    "eventID": "901e25af-0a1c-1234-60a8-2b097c972834",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```


1. Threat actor obtains credentials with IAMFullAccess permissions from GitHub repository

2. Two new users were created to impersonate valid employees

3. IAM policy attached to new users with over-permissive permissions

4. New access keys were generated for the new users

Discovery & Impact

```
All your data is a backed up. You must pay 2.0 BTC to
sXxjVI63R6FaiuIyO93W4t4A60WuWkBMwg 48 hours for recover it. After 48 hours expiration
we will leaked and exposed all your data. In case of refusal to pay, we will contact
the General Data Protection Regulation, GDPR and notify them that you store user data
in an open form and is not safe. Under the rules of the law, you face a heavy fine or
arrest and your base dump will be dropped from our server! You can buy bitcoin here,
does not take much time to buy https://localbitcoins.com with this guide
https://localbitcoins.com/guides/how-to-buy-bitcoins After paying write to me in the
mail with your DB IP: threat@actor.xd
```

1. **Utilizing the compromised accounts, threat actor executes numerous API calls**

2. **Threat actor identified a database through DescribeDBInstances**

3. **Through a VM Instance, threat actor connected to DB**

4. **All databases were dropped and ransomware note was left behind**

Lessons Learned

SECTOR

Overly permissive SCM IAM

The engineer doesn't need access to the entire company's repositories

Credential leak

Credentials should never be committed to SCM

Logging not enabled

Insufficient database and storage bucket loggings made forensic difficult

---

The median ransomware demand in 2022 was

$650,000.

Conclusion

SECTOR

1. Cloud Attack surface grow with new features and workloads
2. Threat actors are getting smarter and more powerful
3. The wide adoption of OSS in the cloud pose hidden risks
4. The industry will see a move away from point security solutions to CNAPPs

SECTOR
BRIEFINGS

Thank you

cloudthreat.report