SECURING IDENTITY AND ACCESS IN THE PUBLIC CLOUD

October 2020

ermetic

Shai Morag
CEO & Co-founder
Ermetic

Background

- CEO & Co-founder @ Secdo - Acquired by Palo Alto Networks for $100M
- CEO @ Integrity Project – Acquired by Mellanox
- Officer @ 8200 - specializing in Cyber Security
- Talpiot Graduate

ermetic

The Public Cloud is key to Digital Transformation

Public Cloud is a Huge Opportunity

- Market Size > $100B
- CAGR > 17%
- Accelerate time to market
- Changing the way we develop Software

ermetic

But every change has a price

Early data breaches had obvious causes

Failing to secure the CSP control plane

Code Spaces

- In June 2014, the AWS account of Code Spaces was compromised
- The company failed to protect its administrative console with multi-factor authentication
- The business was forced to close after the destruction of its assets

THE DEEP END

By Paul Venezia, Senior Contributing Editor, InfoWorld | JUN 23, 2014

Murder in the Amazon cloud

The demise of Code Spaces at the hands of an attacker shows that, in the cloud, off-site backups and separation of services could be key to survival

ermetic

But every change has a price

HONDA experian alteryx accenture

Leaving sensitive S3 buckets publicly accessible

- Alteryx exposed an AWS S3 bucket containing private data of 123 million American households (the data set belonged to Experian which sold the data to Alteryx, a marketing firm)
- Accenture left four AWS S3 buckets unsecured, exposing highly sensitive passwords and secret keys
- Honda left a trove of data stored on two unsecured, publicly accessible and unprotected AWS S3 Buckets

ZDNet CXO HARDWARE MICROSOFT STORAGE INNOVATION APPLE SECURITY MORE NEWSLETTERS ALL WRITERS

Accenture left a huge trove of highly sensitive data on exposed servers

The four exposed servers had no password, but contained the "keys to the kingdom."

Basic configuration errors left data exposed

ermetic

And the proliferation of IaaS/PaaS resources introduces new risks

But every change has a price

VOIPO EXACTIS LevelOne Robotics and Controls, inc.

Exposing sensitive databases

- Voipo exposed a database that contained call and message logs dating back 3 years
- Exactis left an Elasticsearch database publicly accessible, resulting in a breach of PII of 230 million U.S. consumers
- Level One Robotics, exposed sensitive proprietary information of more than 100 manufacturing companies, through a server that allowed unauthenticated data transfer to any rsync client

SC MEDIA

July 23, 2018

Tesla, VW data was left exposed by supply chain vendor Level One Robotics

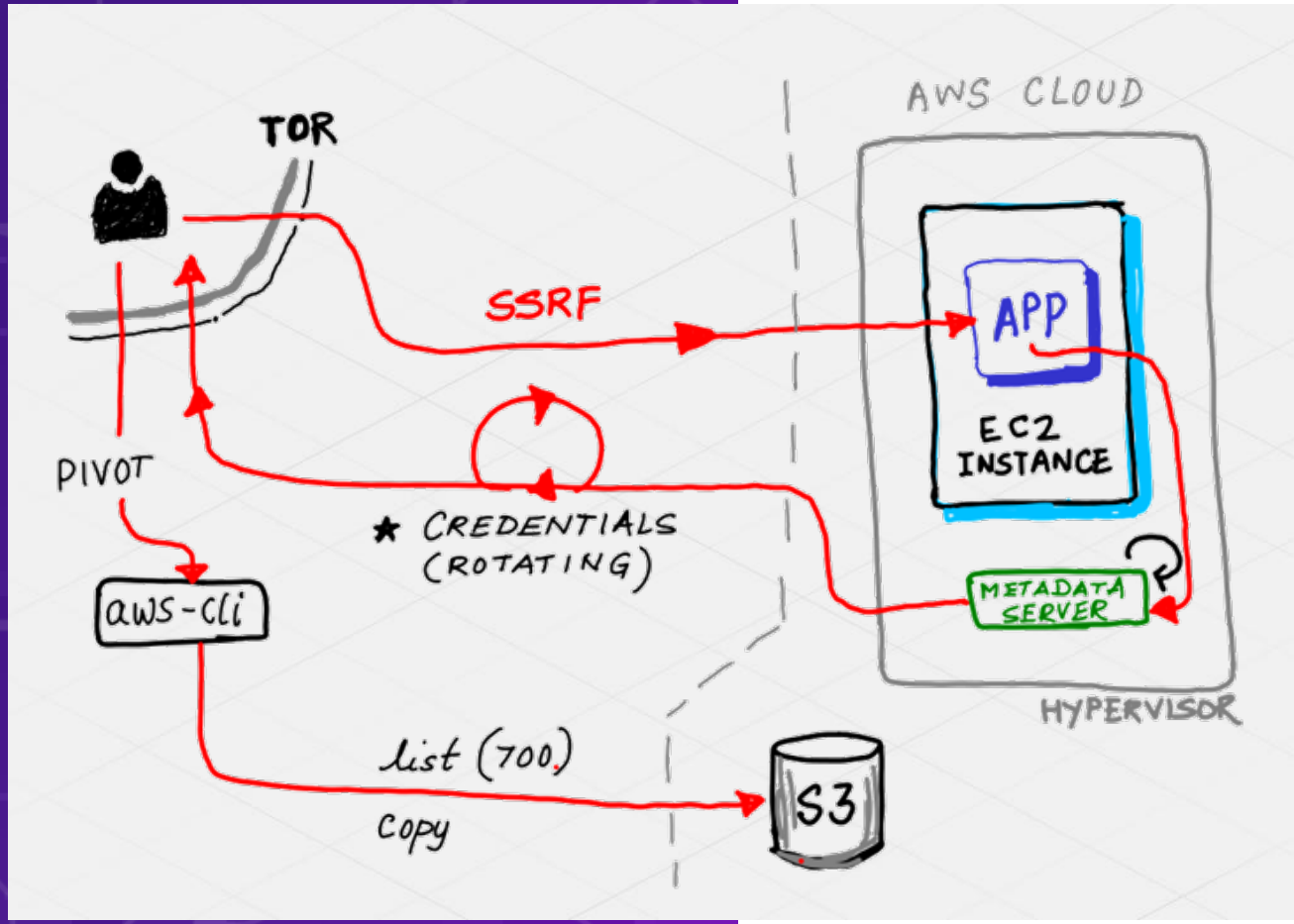
ermetic

Capital One

CASE STUDY

Poor Access Controls Lead to Cloud Breaches

- Compromised Machine
- Excessive access
- No perimeter



ermetic

It’s all about Entitlements & Privileges

“By 2023, 75% of security failures will result from mismanagement of identities, access & privileges”

Gartner, 2020

ermetic

A CLOUD SECURITY PLATFORM, PROVIDING
CLOUD IDENTITY & ACCESS GOVERNANCE

AND SOLVING THE GREATEST
SECURITY CHALLENGES

THROUGH
CONTINOUS ANALYTICS
AND
AUTOMATION

ermetic

ERMETIC

- FOUNDED EARLY 2019
- PALO ALTO, BOSTON & TEL-AVIV
- RAISED ~30M USD (ACCEL, NVP, GCP, TG)
- DOZENS OF CUSTOMER DEPLOYMENTS
- UNIQUE & EXPERIENCED LEADRSHIP TEAM

THANK YOU