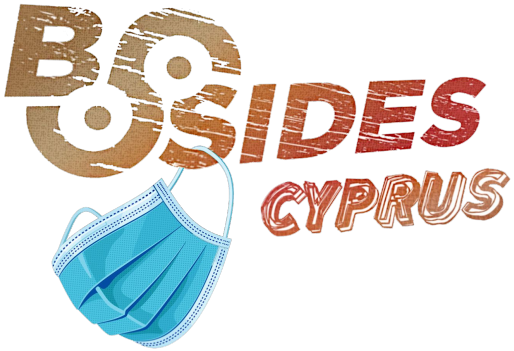
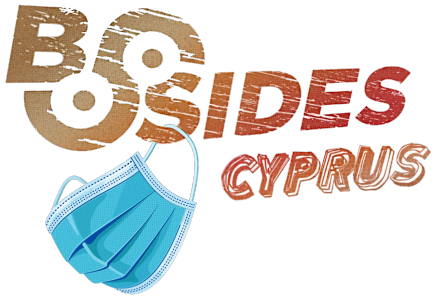


Cloud…
Just somebody else's computer

Anastasios Pingios

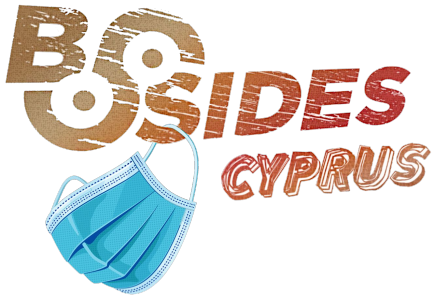
09 October 2021

Disclaimer



All opinions expressed are my own, and do not represent my employer.

whoami



Principal Security Engineer

MITRE Contributor at the ATT&CK framework

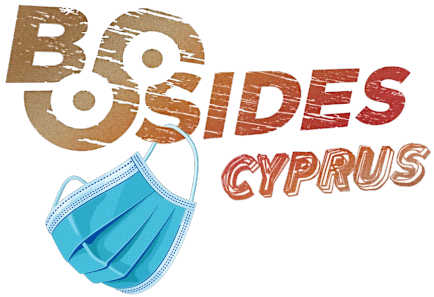
@xorlgr / xorl.wordpress.com

Experience with multiple public clouds

Agenda

BSIDES CYPRUS

Agenda



- Definitions
- Case studies
  - AWS
  - GCP
  - Azure
- Key Takeaways

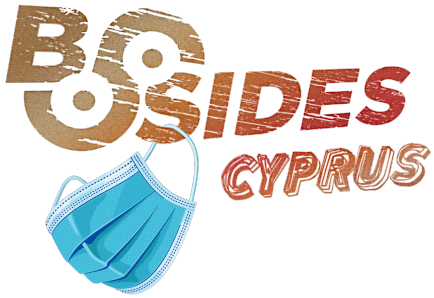
Definitions

BSIDES CYPRUS

Definitions

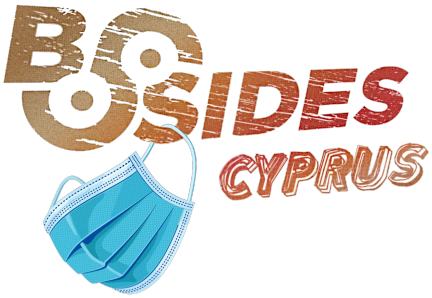
- **Cloud Computing**
  - Introduced as a marketing term in 1996 by Compaq Computer executives to describe the future of internet businesses
  - 1997 trademark application for “Cloud Computing” by NetCentric (defunct)
  - Became popular in 2006 by Google CEO Eric Schmidt, describing shared compute resources as a web service

Definitions



- **Cloud… Just somebody else's computer**
  - Unknown author
  - Became popular joke in 2013-20114
  - Used to describe the early days of basic cloud compute services

Definitions



- **Cloud… Just somebody else's computer**
  - Unknown author
  - Became popular joke in 2013-2014
  - Used to describe the early days of basic cloud compute services

But is it valid?

Case Study

BSIDES CYPRUS

AWS

AWS Case Study

- **2000-2005**
  - Strategic decision to provide an e-commerce as a service platform for third party retailers

- **2006-2010**
  - Started by offering simple infrastructure (e.g. Virtual Machines, network attached storage)

- **Today**
  - Largest customer of AWS is… Amazon!

AWS Case Study

AWS Lambda is an event-driven, serverless computing platform

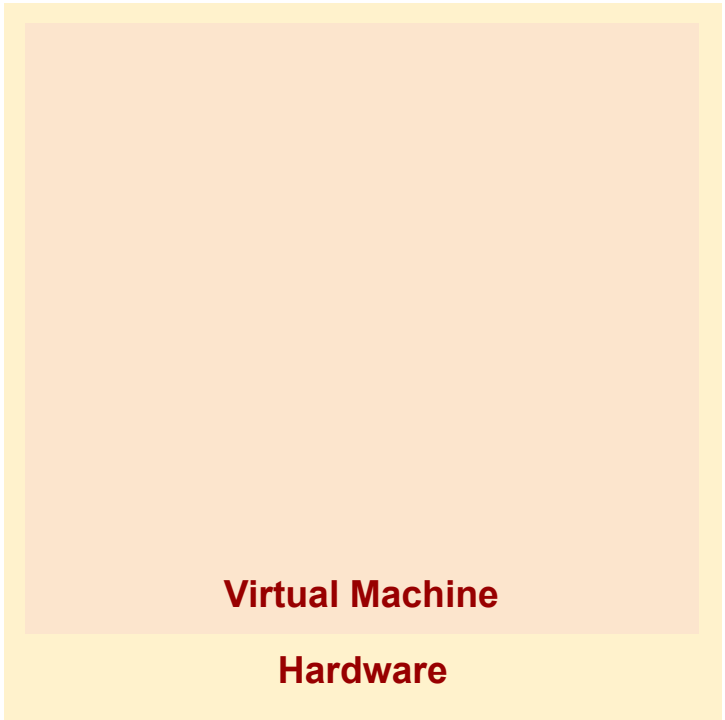
AWS Case Study

Hardware

Sources:

- https://www.denialof.services/lambda/
- SANS: Attacking Serverless Servers: Reverse Engineering the AWS, Azure, and GCP Function Runtime

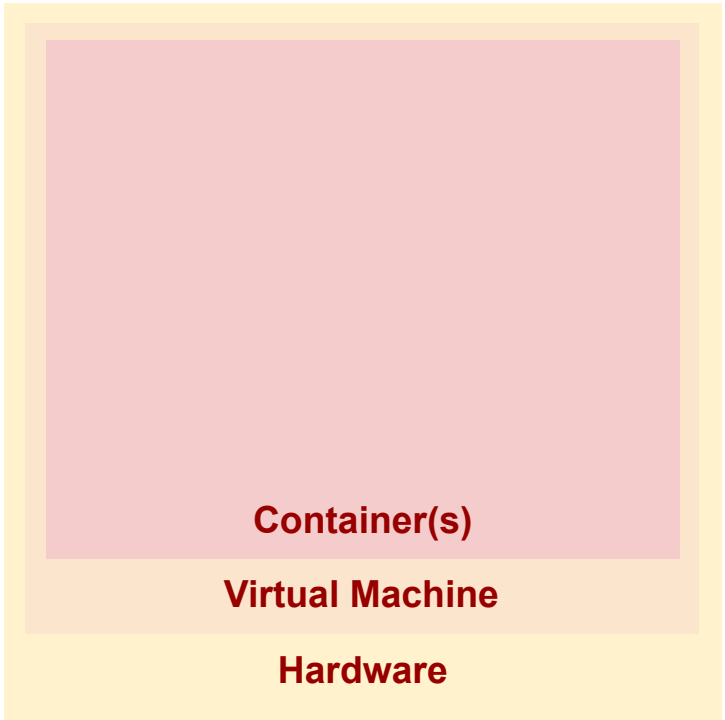
AWS Case Study



Sources:

- https://www.denialof.services/lambda/
- SANS: Attacking Serverless Servers: Reverse Engineering the AWS, Azure, and GCP Function Runtime

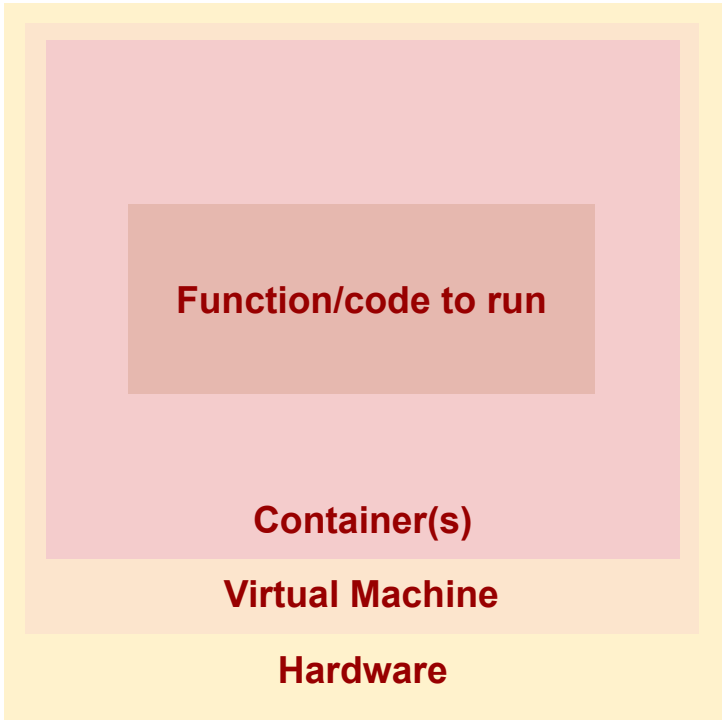
AWS Case Study



Sources:

- https://www.denialof.services/lambda/
- SANS: Attacking Serverless Servers: Reverse Engineering the AWS, Azure, and GCP Function Runtime

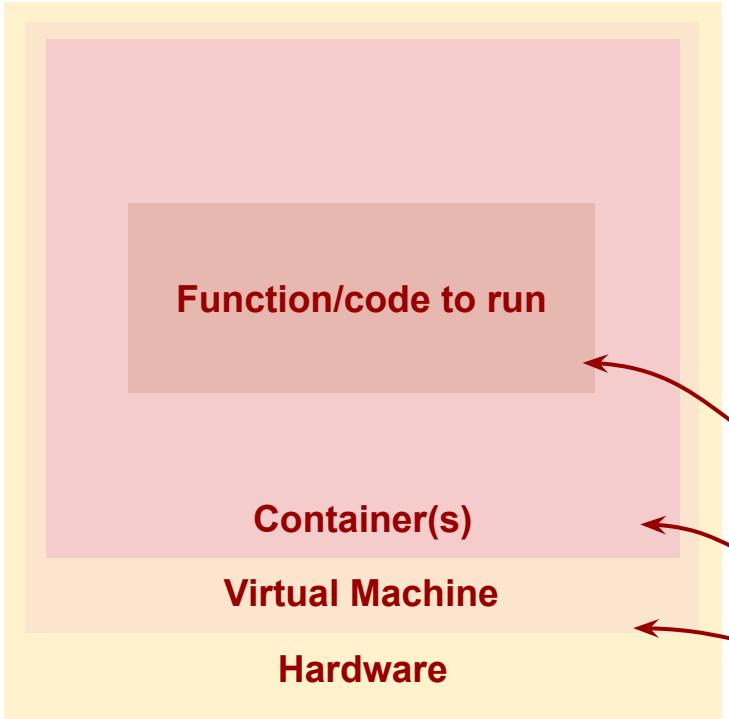
AWS Case Study



Sources:

- https://www.denialof.services/lambda/
- SANS: Attacking Serverless Servers: Reverse Engineering the AWS, Azure, and GCP Function Runtime

AWS Case Study




```
$ lcmd cat /var/runtime/awslambda/bootstrap.py
# -*- coding: utf-8 -*-
"""
aws_lambda.bootstrap.py
Amazon Lambda

Copyright (c) 2013 Amazon. All rights reserved.

Lambda runtime implemention
"""
from __future__ import print_function

import decimal
... snipped for readability
import traceback

import runtime as lambda_runtime

import wsgi


def _get_handlers(handler, mode):
    lambda_runtime.report_user_init_start()
    init_handler = lambda: None

    """
    This is the old way we were loading modules.
    It was causing intermittent build failures for unknown reasons.
    Using the imp module seems to remove these failures.
    """
```

Docker instance of Amazon Linux AMI with a Python parser (`/var/runtime/awslambda/bootstrap.py`)

Kubernetes and Docker (customized) - AWS EKS

KVM (customized) - AWS EC2

Sources:

- https://www.denialof.services/lambda/
- SANS: Attacking Serverless Servers: Reverse Engineering the AWS, Azure, and GCP Function Runtime

AWS Case Study

CloudFront is a content delivery network operated by AWS

AWS Case Study

Source:

- https://disloops.com/cloudfront-hijacking/

AWS Case Study

Anastasios Pingios @xorlgr · Jan 25, 2019
TIL: Amazon has a massive vulnerability (design flaw) that I would call "AWS DNS hijacking-as-a-service"and somehow they managed to get away without even identifying it as one (not even talking about fixing it...). Nice writeup: disloops.com/cloudfront-hij...
2 17 18

Scott Piper @0xdabbad00 · Jan 25, 2019
AWS fixed this issue at some point after that article.
2 2

Anastasios Pingios @xorlgr · Jan 25, 2019
Are you sure? Tested yesterday and seemed to have worked just fine.
1

Scott Piper @0xdabbad00 · Jan 25, 2019
See

cloudfront takeover is not possible anymore · Issu...
AWS finally started mitigating subdomain takeovers on CloudFront. When you try to register Alias ...
github.com

1

Anastasios Pingios
@xorlgr

Replying to @0xdabbad00

This only works if the victim has a Cloudfront set up for {sub-,}domain. If the victim is not using AWS at all the attack still works. Think of Fortune 100 companies with hundreds of thousands of domains + new company acquisitions, many of them never being in the cloud... :(

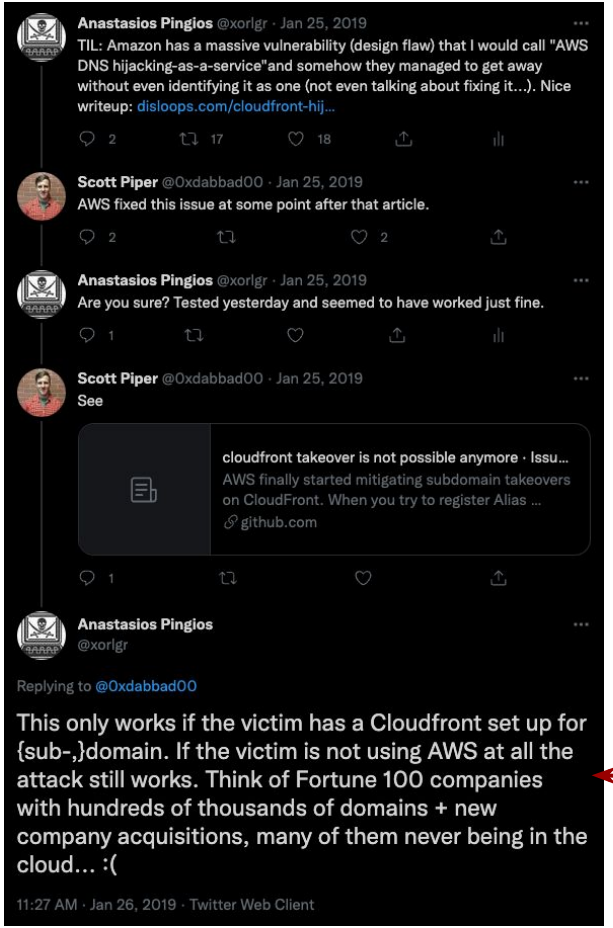
11:27 AM · Jan 26, 2019 · Twitter Web Client

Accidentally publicly leaked a Cloudfront 0day

Source:

- https://disloops.com/cloudfront-hijacking/

AWS Case Study



Anastasios Pingios @xorlgr · Jan 25, 2019
TIL: Amazon has a massive vulnerability (design flaw) that I would call "AWS DNS hijacking-as-a-service"and somehow they managed to get away without even identifying it as one (not even talking about fixing it...). Nice writeup: disloops.com/cloudfront-hij...
2 17 18

Scott Piper @0xdabbad00 · Jan 25, 2019
AWS fixed this issue at some point after that article.
2 2

Anastasios Pingios @xorlgr · Jan 25, 2019
Are you sure? Tested yesterday and seemed to have worked just fine.
1

Scott Piper @0xdabbad00 · Jan 25, 2019
See

cloudfront takeover is not possible anymore · Issu...
AWS finally started mitigating subdomain takeovers on CloudFront. When you try to register Alias ...
github.com

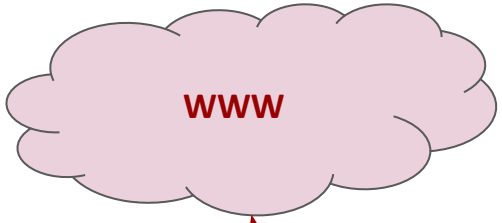
1

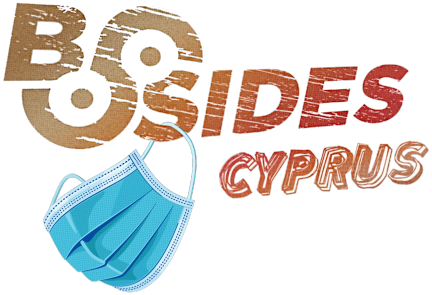
Anastasios Pingios
@xorlgr

Replying to @0xdabbad00

This only works if the victim has a Cloudfront set up for {sub-,}domain. If the victim is not using AWS at all the attack still works. Think of Fortune 100 companies with hundreds of thousands of domains + new company acquisitions, many of them never being in the cloud... :(

11:27 AM · Jan 26, 2019 · Twitter Web Client





Cloudfront CDN

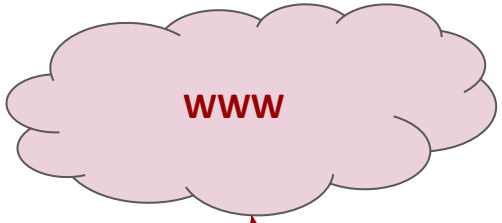
User A
Some web service at example.com

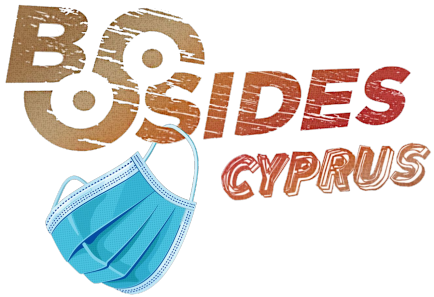
Accidentally publicly leaked a Cloudfront 0day

Source:

- https://disloops.com/cloudfront-hijacking/

AWS Case Study





Cloudfront CDN

Distribution
a.cloudfront.com
to example.com

User A
Some web service
at a.example.com

Accidentally publicly leaked a Cloudfront 0day

Source:

- https://disloops.com/cloudfront-hijacking/

AWS Case Study

Anastasios Pingios @xorlgr · Jan 25, 2019
TIL: Amazon has a massive vulnerability (design flaw) that I would call "AWS DNS hijacking-as-a-service"and somehow they managed to get away without even identifying it as one (not even talking about fixing it...). Nice writeup: disloops.com/cloudfront-hij...
2 17 18

Scott Piper @0xdabbad00 · Jan 25, 2019
AWS fixed this issue at some point after that article.
2 2

Anastasios Pingios @xorlgr · Jan 25, 2019
Are you sure? Tested yesterday and seemed to have worked just fine.
1

Scott Piper @0xdabbad00 · Jan 25, 2019
See

cloudfront takeover is not possible anymore · Issu...
AWS finally started mitigating subdomain takeovers on CloudFront. When you try to register Alias ...
github.com

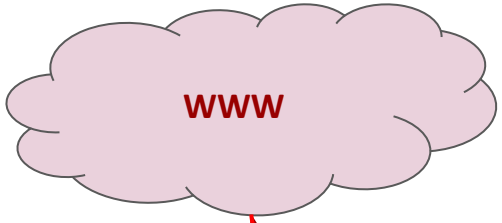
1

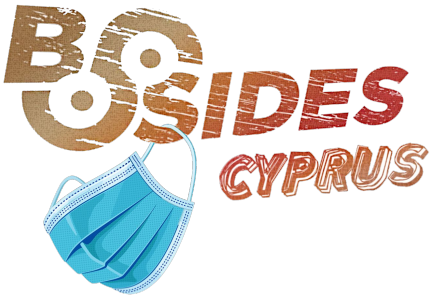
Anastasios Pingios
@xorlgr

Replying to @0xdabbad00

This only works if the victim has a Cloudfront set up for {sub-,}domain. If the victim is not using AWS at all the attack still works. Think of Fortune 100 companies with hundreds of thousands of domains + new company acquisitions, many of them never being in the cloud... :(

11:27 AM · Jan 26, 2019 · Twitter Web Client





Cloudfront CDN

Map the a.example.com CNAME to my distribution

Distribution a.cloudfront.com to example.com

User B

User A
Some web service at a.example.com

Accidentally publicly leaked a Cloudfront 0day

Source:

- https://disloops.com/cloudfront-hijacking/

Case Study

BSIDES CYPRUS

GCP

GCP Case Study

- **2008-2010**
  - Google tried to productionize some of the internally used infrastructure (App Engine)
- **2010-2013**
  - Released several more services to the public cloud
- **Today**
  - Many large customers, but Google has different internal variants for many of those cloud services

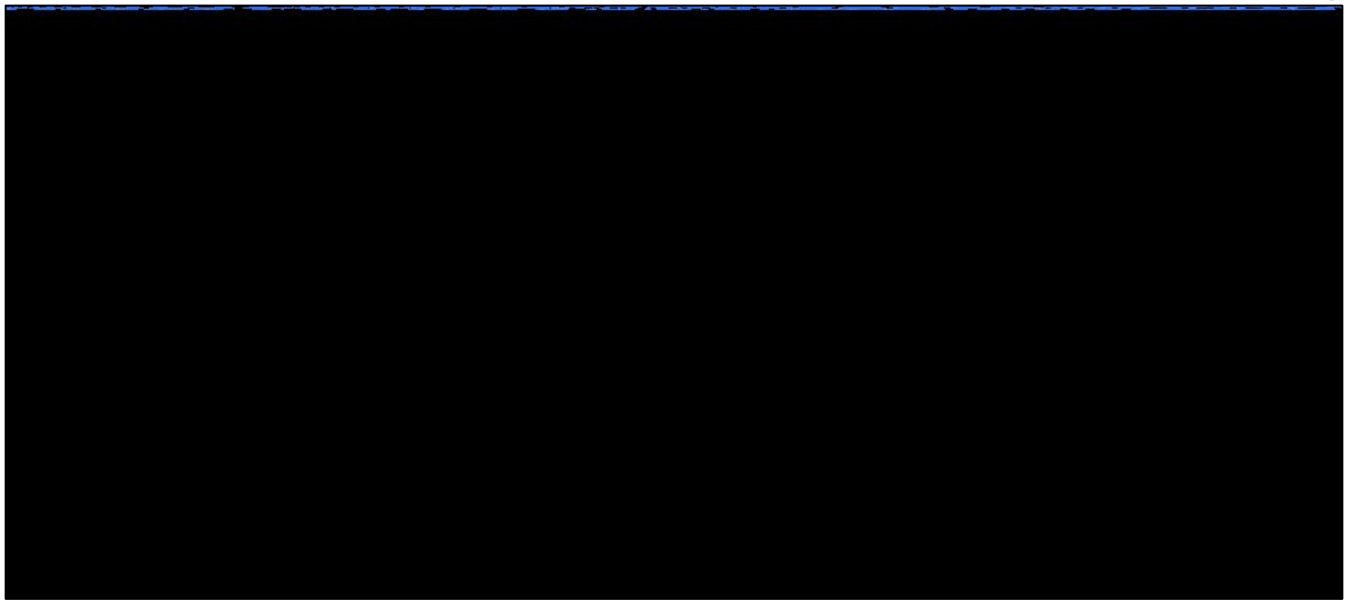
GCP Case Study

Cloud Shell is an online development and operations environment accessible anywhere with your browser.

Source:

- https://89berner.medium.com/persistant-gcp-backdoors-with-googles-cloud-shell-2f75c83096ec

GCP Case Study



Source:

- https://89berner.medium.com/persistant-gcp-backdoors-with-googles-cloud-shell-2f75c83096ec

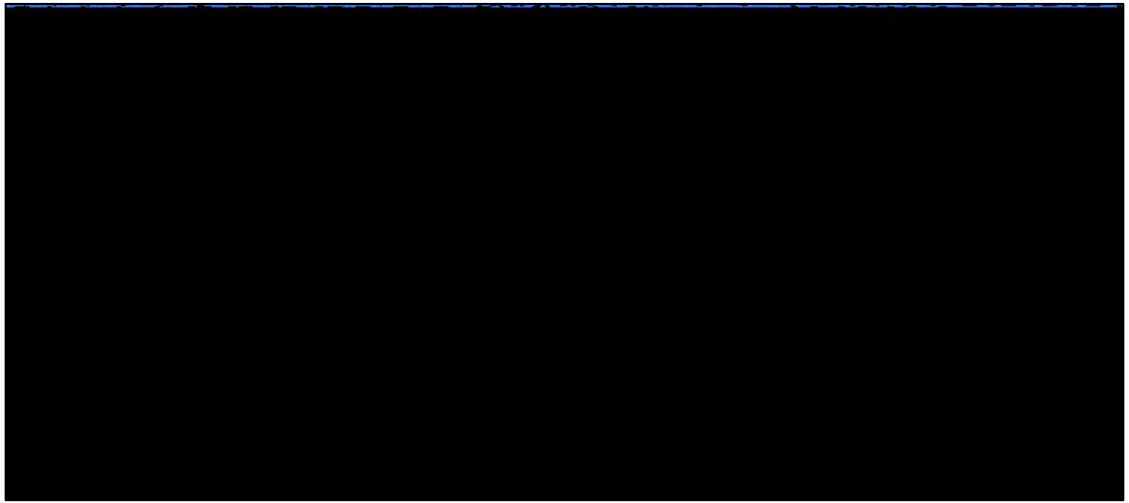
GCP Case Study

Spin up an instance per user after login

Container(s)
(Borg/Kubernetes - GKE)

Virtual Machine (KVM - GCE)

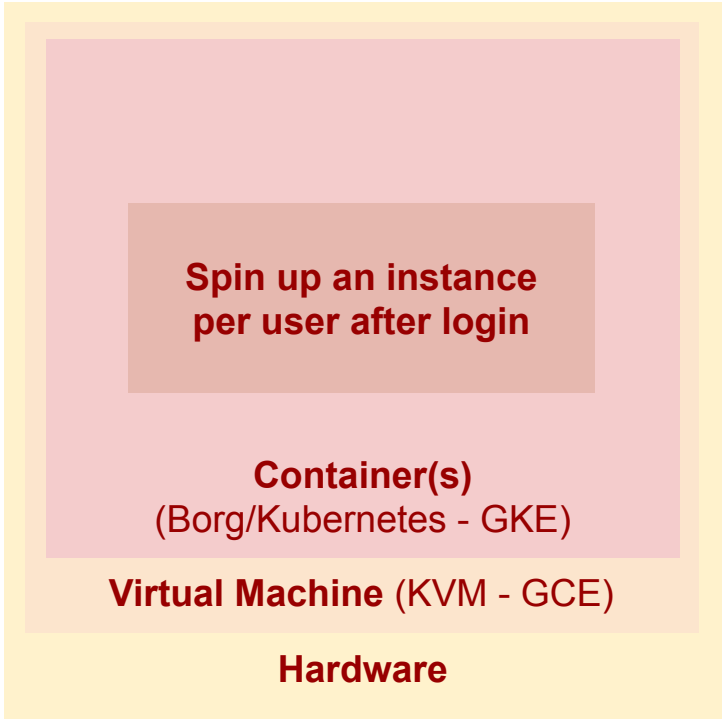
Hardware



Source:

- https://89berner.medium.com/persistant-gcp-backdoors-with-googles-cloud-shell-2f75c83096ec

GCP Case Study



- Persistent container with access to a service account for your user
- **Issues**
  - You can permanently install malware or backdoors there by gcloud command, social engineering, etc.
  - It had no audit or command logging on who executed what
  - It could be used as a C&C for any in-the-project activities through the attached service account

Source:

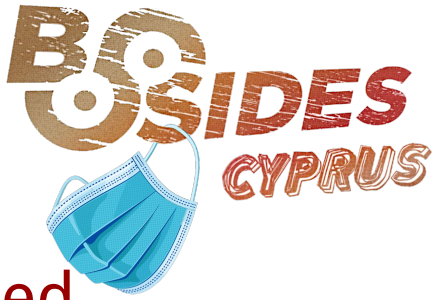
- https://89berner.medium.com/persistant-gcp-backdoors-with-googles-cloud-shell-2f75c83096ec

Case Study

BSIDES CYPRUS

Azure

Azure Case Study



- **2008**
  - Announced officially, internally codenamed Project Red Dog
- **2010**
  - Official release with simple infrastructure services
- **Today**
  - Most of Microsoft internal systems are on Azure
  - Second largest (after AWS) market share

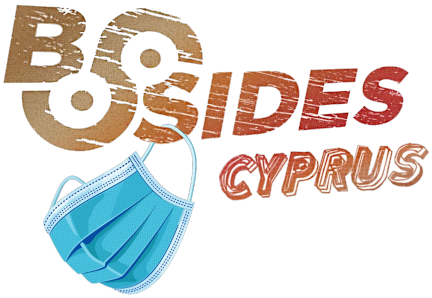
Azure Case Study

The ASDK (Azure Stack Development Kit) is a single-node deployment of Azure Stack Hub that you can download and use for free

Source:

- Microsoft Hybrid Cloud Unleashed with Azure Stack and Azure (2017), ISBN: 9780134301976
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-I/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/

Azure Case Study



User interfaces (web UI, Azure API, etc.)

Resource providers (assign nodes to users, request new storage, etc.)

Management/control layer (manage nodes, storage, networks, deployments, etc.)

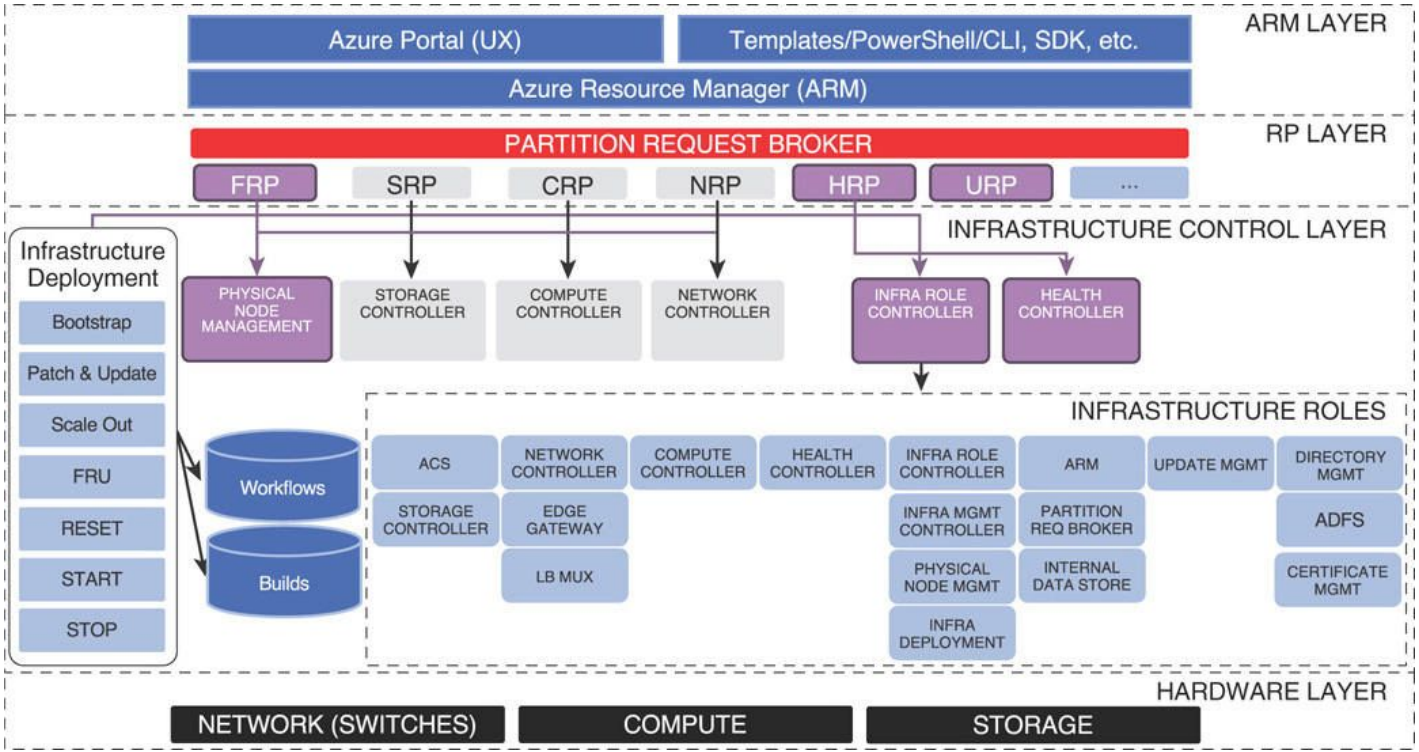
Internal APIs for different operations to the hardware (get info, config HW, etc.)

Hardware (servers, switches, storage, etc.)

Source:

- Microsoft Hybrid Cloud Unleashed with Azure Stack and Azure (2017), ISBN: 9780134301976
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-I/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/

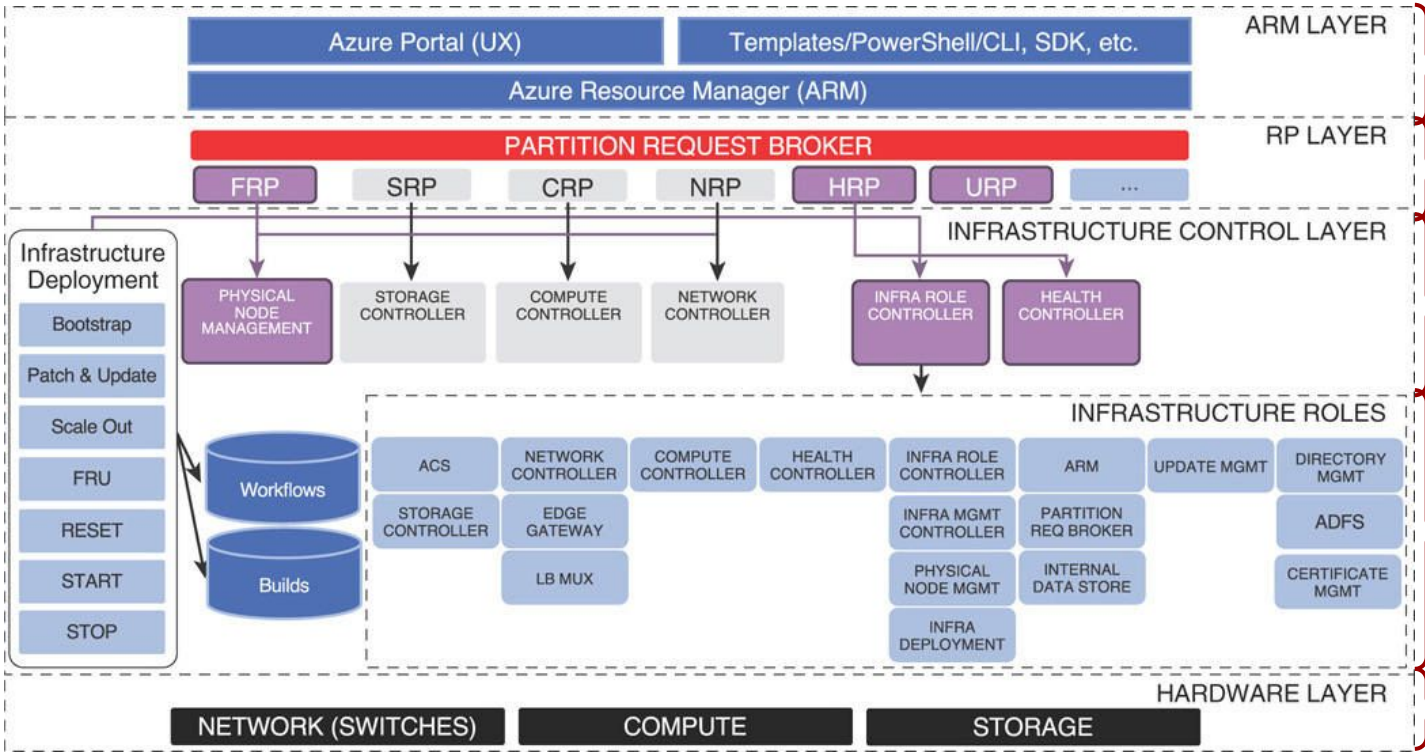
Azure Case Study



Source:

- Microsoft Hybrid Cloud Unleashed with Azure Stack and Azure (2017), ISBN: 9780134301976
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-I/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/

Azure Case Study



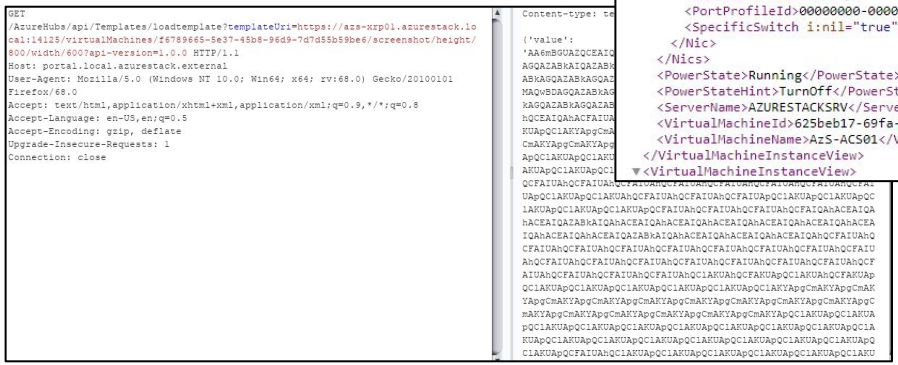
Source:

- Microsoft Hybrid Cloud Unleashed with Azure Stack and Azure (2017), ISBN: 9780134301976
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-I/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/

Azure Case Study

- Checkpoint tested the “Service Fabric Explorer” RP (Resource Provider)

- Found 3 issues* of internal APIs that required no authentication, leaking information of other tenants
  - `QueryVirtualMachineInstanceView`
  - `GetVirtualMachineScreenshot`
  - `GetStringAsync`



And an RCE which I’m not covering here

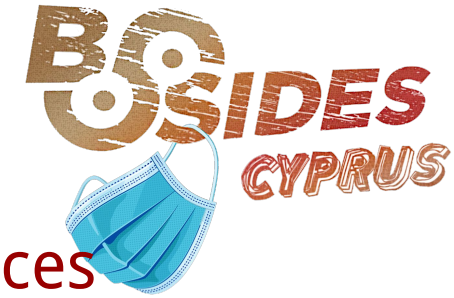
Source:

- Microsoft Hybrid Cloud Unleashed with Azure Stack and Azure (2017), ISBN: 9780134301976
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-I/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/

Key Takeaways

BSIDES CYPRUS

Key Takeaways



- If you remove the abstraction, all cloud services are infrastructure found in many large-scale deployments
- Don’t be discouraged by the buzzwords, abstraction layers, and marketing pitches when doing cloud security
- Public cloud is good, but not panacea. It is built for common use cases, not for corner cases
- Yes… Cloud is just somebody else’s computer…

Thank you!

BSIDES CYPRUS