#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **CSCS-R02**

# It’s Getting Real & Hitting the Fan! Real World Cloud Attacks


**OFER MAOR**

CTO, Mitiga
@OferMaor

MITIGA

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

# Speaker

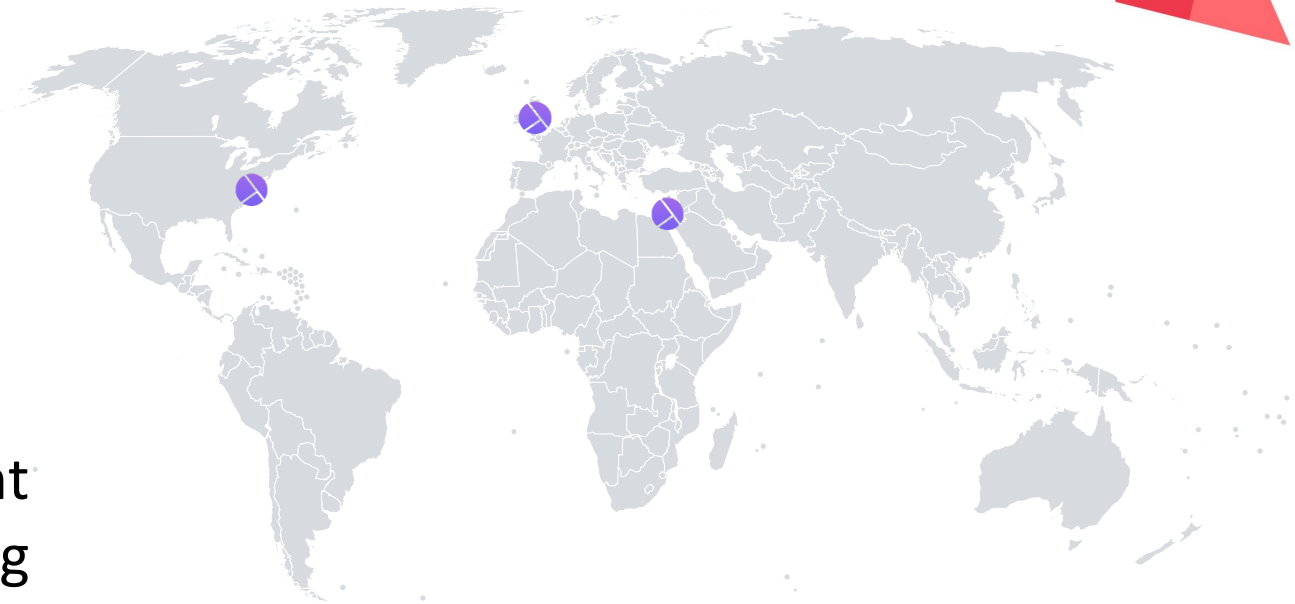
- CTO & Co-Founder, Mitiga
- Over 25 Years in Cybersecurity
- Hacker at Heart
- CloudSec & AppSec *(Daytime)*
- Incident Response *(Nights & Weekends)*
- Pioneer of IAST

@OferMaor

ofer@mitiga.io

Linkedin.com/in/ofermaor

# About Mitiga



Mitiga's mission is to prevent our customers from experiencing a crisis — even during a breach — by providing a proactive next-gen Incident Response solution

- **Forensics Data & Automation**
- **Fastest Time to Recovery**
- **Incident Command Center**
- **Incident Readiness**

- **Breach Investigation Faster than Humanly Possible**
- **Continuous, Proactive Breach Investigation**
- **IR² == Zero Cost Critical Incident Response**

# Introduction

**Breaches are Inevitable**

**World is Moving to the Cloud**

**Cloud Breaches are Here!**

## Today's Talk:

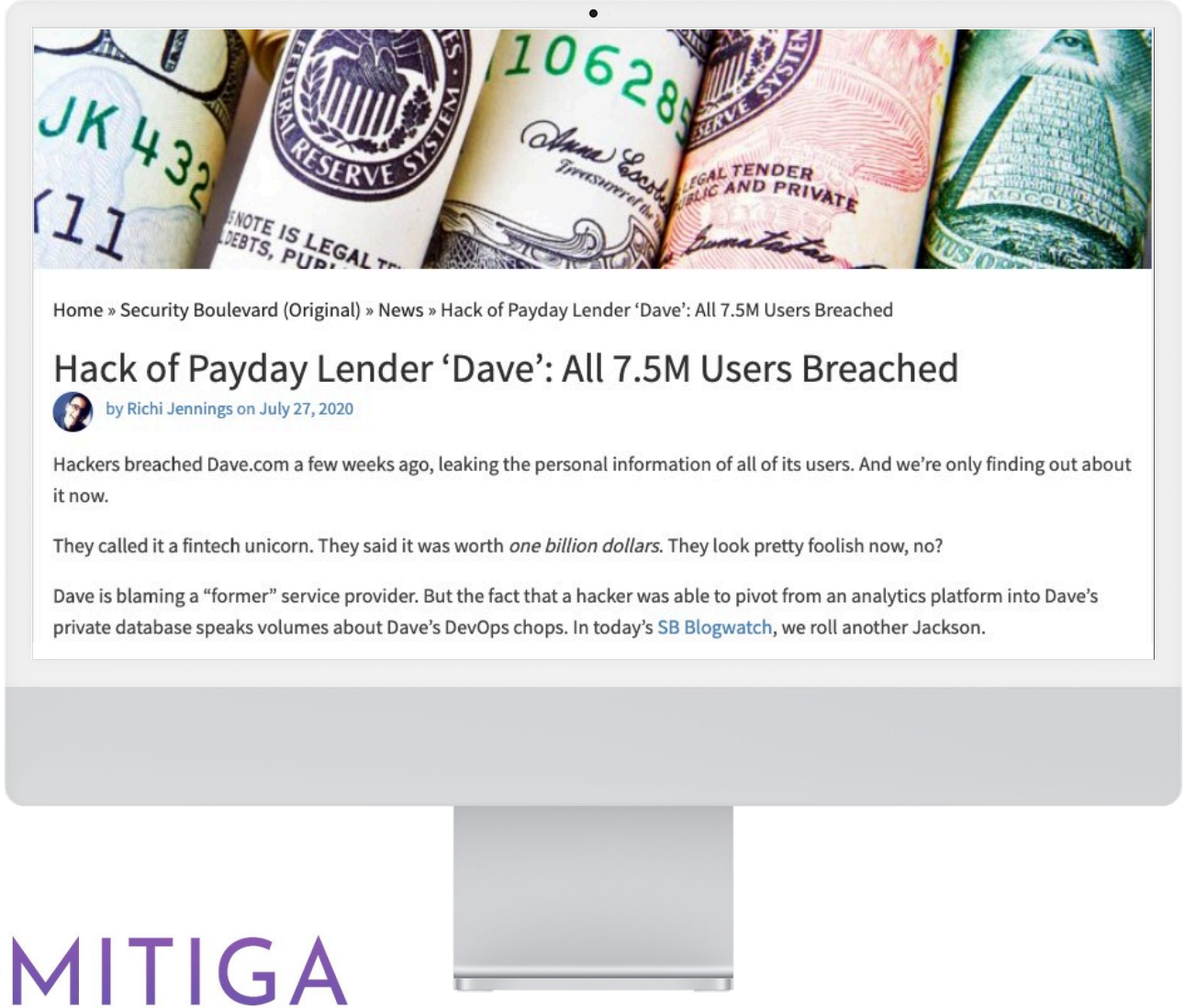
1. Learn about cloud breaches through real world stories
2. Realize how the right breach response can reduce impact and prevent loss
3. Understand what you can today to become more resilient and be ready for breaches

RSAConference2022

# Incident #1:

# From SaaS Marketplace to a Full Breach

# From SaaS Marketplace to Major Breach



Home » Security Boulevard (Original) » News » Hack of Payday Lender 'Dave': All 7.5M Users Breached

## Hack of Payday Lender 'Dave': All 7.5M Users Breached

by Richi Jennings on July 27, 2020

Hackers breached Dave.com a few weeks ago, leaking the personal information of all of its users. And we're only finding out about it now.

They called it a fintech unicorn. They said it was worth *one billion dollars*. They look pretty foolish now, no?

Dave is blaming a "former" service provider. But the fact that a hacker was able to pivot from an analytics platform into Dave's private database speaks volumes about Dave's DevOps chops. In today's SB Blogwatch, we roll another Jackson.

- Dave.com used Waydev code analytics via GitHub Marketplace.
- Waydev was hacked, and through it Dave.com's code was accessed.
- Cleartext secrets in Dave.com code allowed for unauthorized access.
- Data was stolen and leaked on the Darknet.
- DevOps blamed!

MITIGA

# Yet Another Marketplace App Compromised

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Home › Incident Response

## DeepSource Says Hackers Compromised Its GitHub Application

By Ionut Arghire on July 22, 2020

Share Tweet Recommend 1 RSS

**Automated code review tool provider DeepSource this week announced that it reset tokens, secrets, private keys, and employee credentials after being informed that its GitHub application was compromised.**

not been breached," the startup **announced**.

Starting mid-June, the GitHub Security team observed numerous requests from unusual IP addresses for DeepSource users, but was not sure that a compromise had occurred, despite the anomalous traffic.

Following a deeper investigation, however, GitHub determined that hackers managed to compromise the GitHub account of one of DeepSource's employees, as part of the **Sawfish**

MITIGA

# Is it Too Long? Yes, It Is!

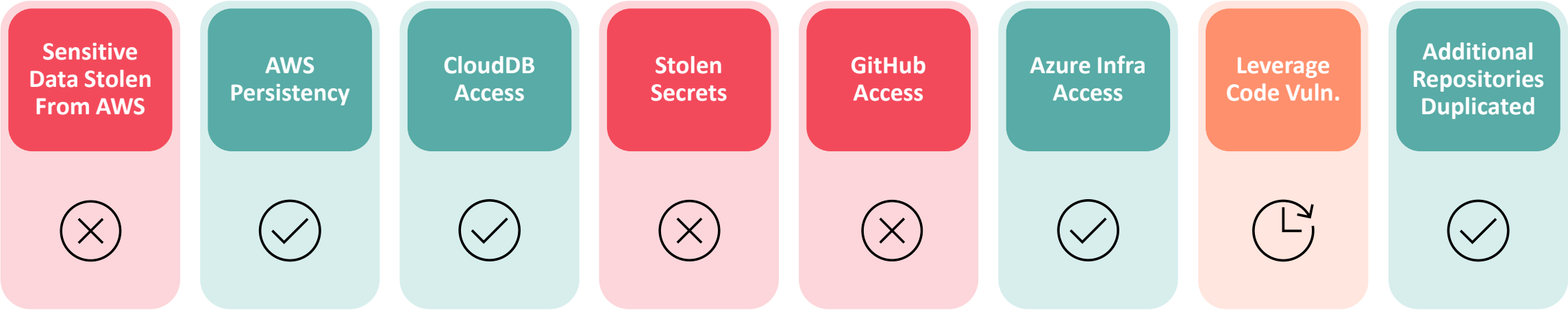
- Partial timeline (obfuscated)
- 3 months (!) between detection and notification
- Another 10 days to notify affected customers!
- Plenty of time for attackers

| | Incident Timeline | Client Activity |
|---|---|---|
| November 20, ‘19 | | DeepSource plugin installation |
| Mid April ‘20 | Phishing incident at DeepSource | |
| May 31, ‘20 | **Code** cloned by **devuser** user from location with IP **X.X.X.X** | |
| July 11, ‘20 | DeepSource were informed of the hack by GitHub | |
| July 21, ‘20 | | Received mail from GitHub and evaluation initiated |
| July 22, ‘20 | | DeepSource key removed from GitHub Account |

MITIGA

# The Response Can Be Long…

- Full investigation, exploring potential abuse by attackers
- Hypothesis based ***Hunting*** mode



# Substantial Impact

- **Source Code Leak** *(Including sensitive AI IP)*
- **AWS Secrets Compromise** *(Some access)*
- **Two Major Customer Disruptions**
  - One customer suspending service for days
  - Second customer initiating massive (and expensive) audit and review
- **Substantial Costs**
- **Increase in Insurance Premium**

RSAConference2022

# Incident #2:

# Redis, Set, Mine!

# Suspicious Files on EC2 Instance

**Malicious files found on servers (18 in total)**

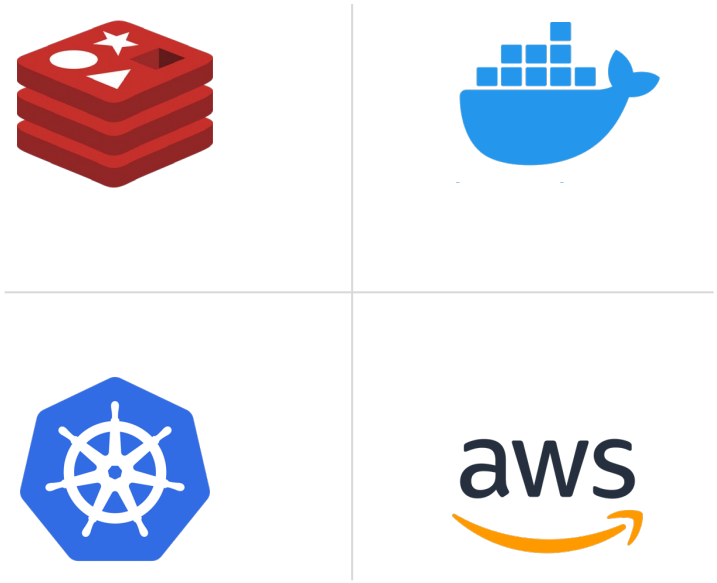
root – md5 hash bdd0aab39e0bd7de2e900fd662bf37f1
zzh – md5 hash ef44c7cb178b0652ad659ee810e07aaf

**ZZH file used to download CryptoMiner**

Bash Script - hxxp://oracle[.]zzhreceive[.]top
IP Addresses – 107.189.3.150 / 199.19.226.117

**TTPs Associated with TeamTNT/Watchdog**

# CryptoMining through Cloud Tech

# The Redis AMI

Initial investigation could not identify any vulnerability as the root cause for the infection

Infected servers correlated to a single AMI

Downloads — ubuntu@ip-[redacted]: ~ — ssh -i ami.[redacted] ubuntu@ec[redacted]...

```
# pwd
/datadb/redis
# dir
backup.db  root  zzh
#
```

**Redis misconfiguration during AMI creation, led to compromise of the source image!**

MITIGA

# Cloud CryptoMining is Big!

# AWS Community AMI with Cryptominer

DARKReading Cloud | 4 MIN READ | ARTICLE

## Cryptominer Found Embedded in AWS Community AMI

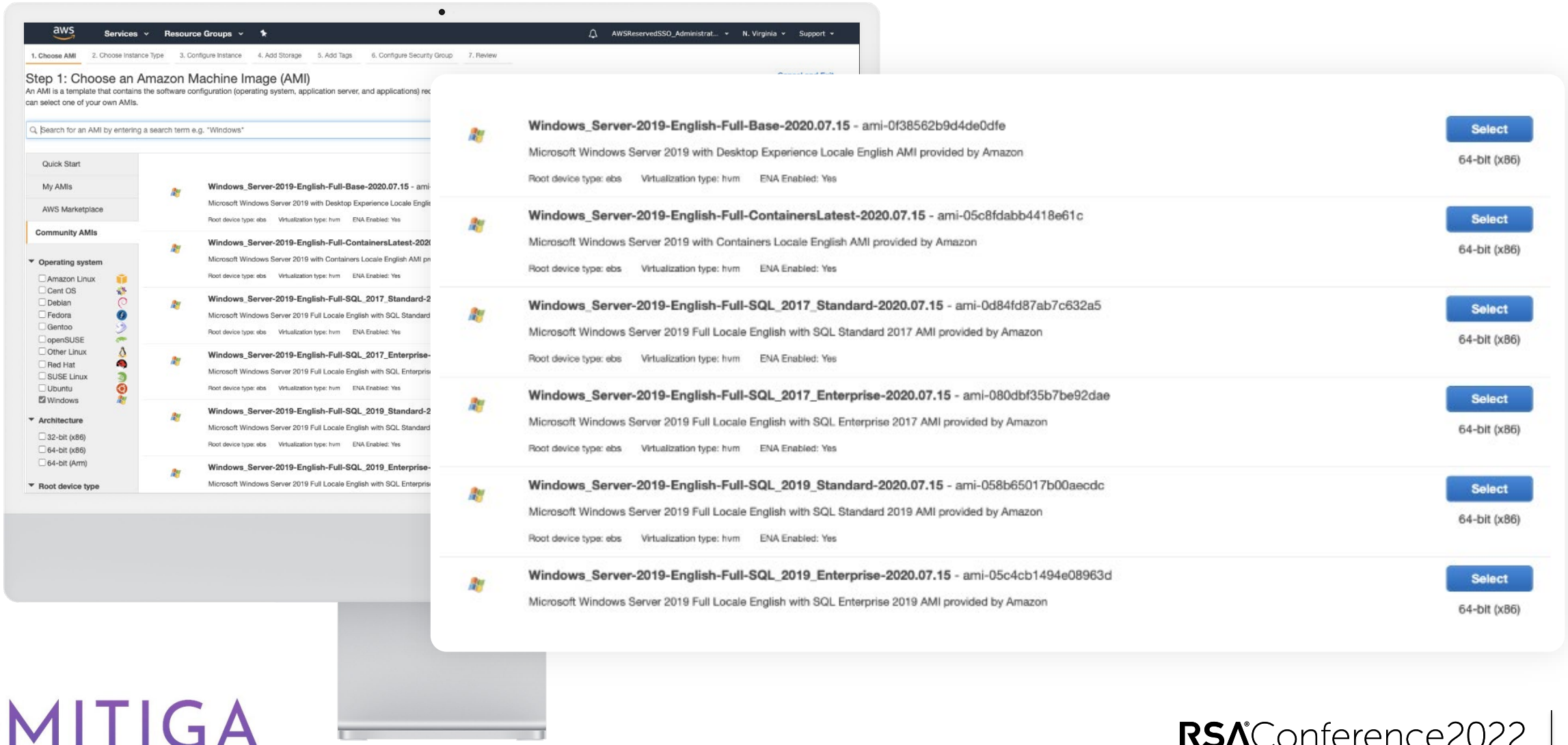
Researchers advise Amazon Web Services users running Community Amazon Machine Images to verify them for potentially malicious code.

**Kelly Sheridan**
Senior Editor

August 21, 2020

Security researchers urge AWS customers running Elastic Cloud Compute (EC2) instances based on community Amazon Machine Images (AMIs) to check for potentially malicious embedded code, following their discovery of a cryptominer lurking inside a Community AMI.

# When You Need Windows 2008 Server AMI…




MITIGA

# Can You Spot the Malicious One?

**Windows_Server-2019-English-Full-Base-2020.07.15** - ami-0f38562b9d4de0dfe

Microsoft Windows Server 2019 with Desktop Experience Locale English AMI provided by Amazon

Root device type: ebs  Virtualization type: hvm  ENA Enabled: Yes

OR

**Amazon/Windows_Server-2008-R2_SP1-English-64Bit-Base-2015.01.02** - ami-1e542176

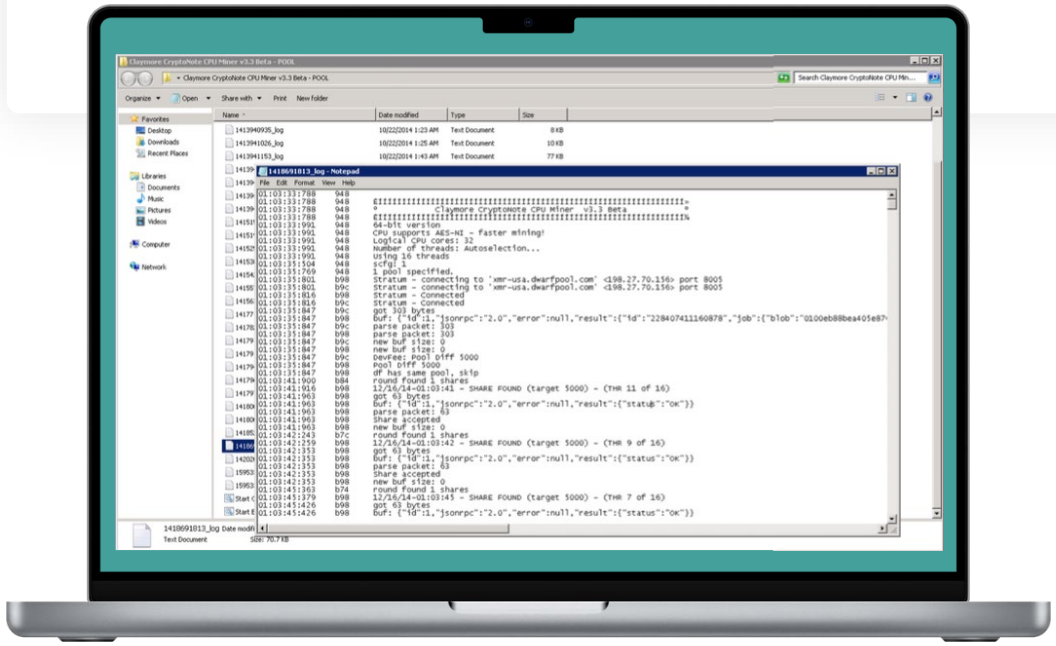
Root device type: ebs  Virtualization type: hvm  ENA Enabled: No

# And When You Can't….

Start Canada - Notepad

File Edit Format View Help

```
NsCpuCNMiner64.exe -o stratum+tcp: //xmr-usa.dwarfpool.com:8005 -u 47sghzufGh] JOQEbScMCwVBimTug6L5J]
iRixD8VeGbp jCTAI 2noXmidZyBZLc 99eGENtNK FF 34 FHsGRoyZk3ES1s1VaQVcB .
6c9472048.a3bfc85b5b27e39058d576e1ac56b7686726efbcd74f93392ae029b -p x
```



MONERO

CryptoMiner

**Siphoning Money**

MITIGA

RSAConference2022

# Incident #3:

# $15M Through O365 Without Leaving Your Couch


CPO MAGAZINE



Alicia Hope

# Fraudsters Steal $15 Million From American Businesses Through a Coordinated BEC Scam

Hackers stole about $15 million between April and September 2020 by targeting over 150 organizations through a business email compromise (BEC) scam, according to an Israeli-based cybersecurity firm Mitiga. The firm revealed that cybercriminals would impersonate senior executives using perceived legitimate Microsoft Office 365 email addresses, and convinced the victims to deposit money in different accounts owned by the criminals.

# Background

## Collector's Item Transaction

**Result:** Over $15M Stolen

### Actors

- Buyer
- Seller
- Threat Actor
- Legal Firm
- Restoration Expert

### Investigation Outcome

- Found evidence of compromise (Buyer)
- Found TTPs, connected to other cases by same cybercriminal group
- US Secret service involved

# Attack Flow

**PRE-SCAM**
April - May

Access to Buyer's O365 mailbox → Forwarding rule & intel gathering → Filtering and folder manipulation → Fake domains registration with O365 account

**SCAM**
May - July

**Man-in-the-Middle communication** → **Money transfer** → **Stalling while maintaining access**

# Over 150 Organizations Impacted!

- Months-long – Combining BEC with Account Compromise
- All email accounts setup on O365 (avoiding discrepancies)
- Forwarding Rules set to track all activity
- Filtering Rules moving mails to concealed folders
- Rogue domains registered on Wild West Domains
  (Similar patterns revealing over 150 additional fake domains)

# Interactive TTPs – Registration Pattern

**Registrar** Wild West Domains (owned by GoDaddy)

**Nameserver** Microsoft

**TXT records** O365 account with a unique Microsoft Identifier (strong) or with similar TTPs (medium)

**PRE-SCAM** April - May → Access to Buyer's O365 mailbox → Forwarding rule & intel gathering → Filtering and folder manipulation → Fake domains registration with O365 account

**SCAM** May - July → **Man-in-the-Middle communication** → **Money transfer** → **Stalling while maintaining access**

RSAConference2022

# Incident #4:

# MongoDB Ransomware Extortion

# Good Morning – Your Data is Gone!

Entire MongoDB Erased

MongoDB Data Stolen, Replaced with Ransom Note:

All your data is a backed up. You must pay 4 BTC to 1MFYW2zGnscSDyjsPBUYTjmY4zrzZCfQHa 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: recoverdb@mailnesia[.]com and you will receive a link to download your database dump.

# Investigation Trail

**November 25**

20:44:53.890 (UTC) – MongoDB Service Binded to 0.0.0.0

**November 27 – Connections from TOR Exit Node**

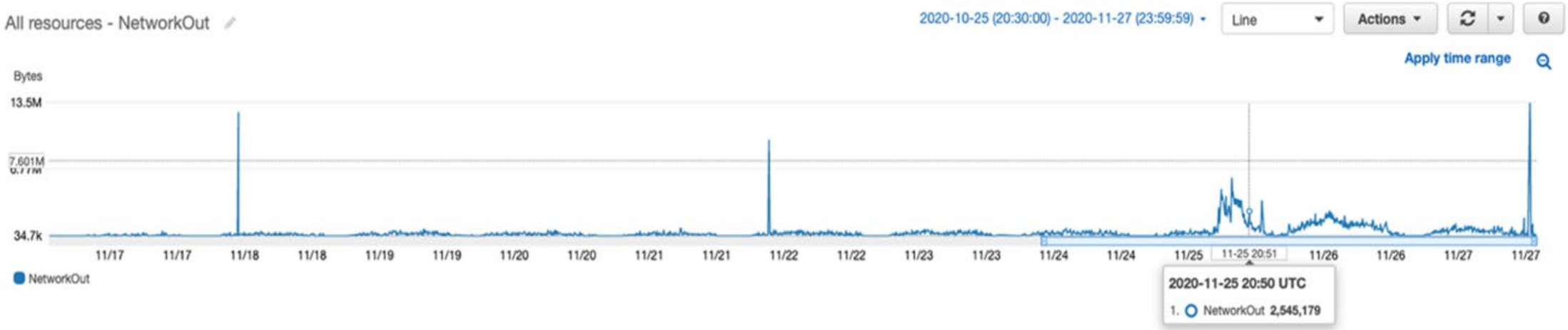
| | |
|---|---|
| 17:54:51 → 17:54:54 (UTC) | *// Recon* |
| 17:54:56 → 17:54:57 (UTC) | *// Create collection (READ_ME_TO_RECOVER)* |
| 17:54:59 → 17:55:03 (UTC) | *// Created ransomware document* |
| 17:55:04 → 17:55:06 (UTC) | *// Deleted Database* |

✕ **Poor MongoDB Log Configuration - Limiting Investigation Confidence**

# Lucky Break!

Customer had full Backups!

Forensics investigation proved no actual data leak (!)




**Ransom payment prevented.** This time…

MITIGA

RSAConference2022

# Incident #5:

# From On-Prem AD to Full Blown Cloud Attack

# Yet Another Ransomware?

**7 x**

**EC2 Servers Encrypted**

README.txt - Notepad

File Edit Format View Help

## Double Ransomware Note (readme.txt)

- Decryption (not needed, backups available)
- Data Leakage

# Root Cause Analysis

**April 30**

**TA encrypts, leaving readme.txt ransom note**

**April 15**

**TA runs rclone.exe to exfiltrate data to MEGA.nz**

**April 5-14**

**Lateral movement, gaining access to all 7 servers**

- Leveraging OktaService account
- Connecting via decomissioned VPN from on-prem DC to AWS Environment
- Deployment of various tools for exploit and persistency

**April 1**

**TA takes over on-prem DC**

- Compromised administrative employee account
- Attempts MFA challenges till employee approves
- Takes over the OktaService account

# Containment & Recovery

## Servers Recovery

- Snapshot restoration (14 days back) restored to compromised environment
- Rebuilt servers from clean images
- Recovered database from dedicated Database backup

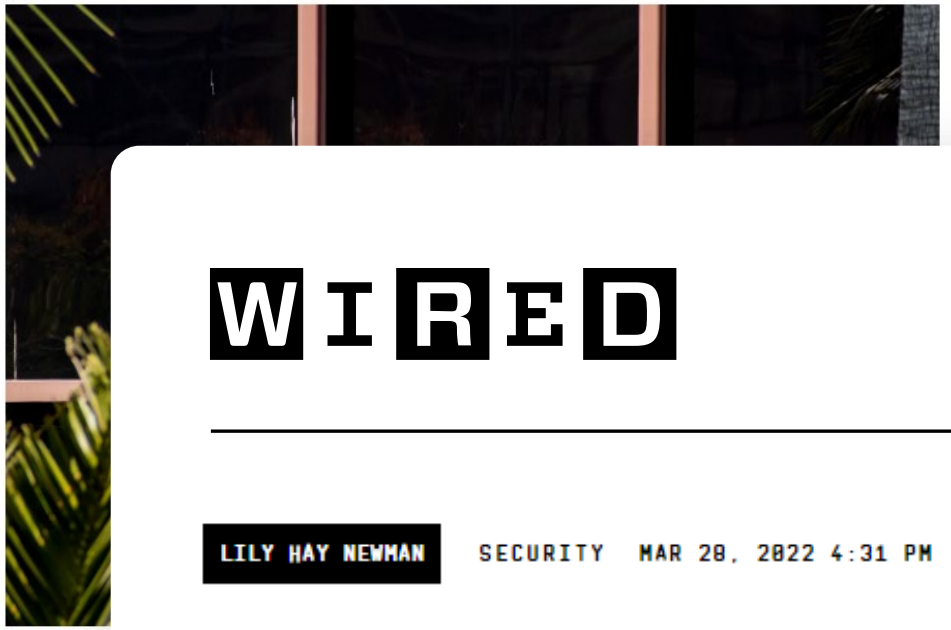
## Data Leakage Containment

- Analysis of data leakage identified operating credentials of TA's server
- All data leaked downloaded and analyzed for identification of PII and Sensitive Data
- Finally, data erased from TA's server!

**No Ransomware Paid!**

RSAConference2022

# Some Thoughts on Okta (And Critical SaaS)



PHOTOGRAPH

IN THE W
breached
company
have bee
subproce

WIRED

LILY HAY NEWMAN SECURITY MAR 28, 2022 4:31 PM

# Leaked Details of the Lapsus$ Hack Make Okta's Slow Response Look More Bizarre

Documents shed some light on how Okta and its subprocessor Sitel reacted to a breach, but they don't explain the apparent lack of urgency.

# SaaS Breaches Are Here!

The okta Breach was just a reminder.

## SaaS Breaches are Challenging!

- ✕ You only have partial control
- ✕ You may lack the relevant forensics data
- ✕ You may lack the skill needed to investigate
- ✕ Each platform has different capabilities

**It goes straight to high value targets**

okta salesforce

slack Office 365

... etc.

RSAConference2022

# Key Takeaways!

# So, What Can We Do?

**Breaches are Inevitable**

**World is moving to the Cloud**

**Cloud Breaches are Here!**

### 1 Learn

Continue learning about actual cloud breaches to allow for better prevention, detection and response

### 2 Prepare

Create the right plans, tools capabilities and team, to be ready to deal with cloud breaches when they occur

### 3 Respond

Deploy fast and efficient Incident Response tech and teams to reduce impact and prevent loss

RSAConference2022

# THANK YOU!

Ofer Maor

CTO
Mitiga
@OferMaor