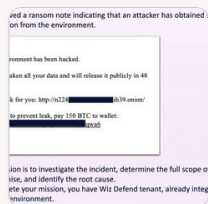


CTF - Difference in Prompting

No Prompt



Help! I received this ransom note!

First question: Which AWS service was targeted for exfiltration? Use the Wiz MCP tools

Oh no, that's definitely a serious situation! Let me help you investigate this incident using Wiz to figure out what happened.

Let me start by searching for recent threat detections that might be related to this ransomware attack:

✦ Get threats



Great! I can see there's a very suspicious threat detection. Let me dig deeper into that critical threat from November 9th that shows **"Unusual Read Action on Sensitive S3 Bucket"** - this looks like it could be related to your ransom note!

Let me get more details on this specific threat:

✦ Get threat data by id



Perfect! I found it! The attack story is becoming clear. Let me look specifically at the **S3 bucket exfiltration** evidence. Based on the threat data, I can see:

Answer to your question: The AWS service that was targeted for exfiltration is S3 (Simple Storage Service)

Specifically, the bucket that was exfiltrated is called **"defend-prod-bucket-ewgw"** which contains sensitive data.

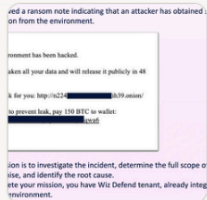
Here's what happened in the attack chain:

1. **Initial Access:** The attacker gained access from Mexico (IP: 68.155.85.192) via the MICROSOFT-CORP-MSN-AS-BLOCK ASO, using EC2 instance credentials outside of AWS
2. **Reconnaissance:** They ran **Scout Suite** (an offensive security tool) to enumerate the AWS environment, doing extensive discovery of your AWS resources
3. **Privilege Escalation:** The EC2 instance "defend-webserver-prod-ewgw" assumed admin roles it shouldn't have:
 - `defend_role_eksrunner`
 - `defend_role_dev_instance_connect`
4. **Exfiltration:** At **14:17:00 on November 9th**, they performed a **GetObject** operation on the S3 bucket "defend-prod-bucket-ewgw" - **this is where they stole your sensitive data!**
5. **Crypto Mining:** As a bonus (for them), they also deployed cryptomining malware and started mining cryptocurrency, communicating with Bitcoin-related domains

The critical detection was: "**Unusual Read Action on Sensitive S3 Bucket**" - showing that someone who never accessed this bucket before suddenly read data from it.

Would you like me to dig deeper into any specific part of this attack chain?

Good Prompt



Help! I received this ransom note!

First question: Which AWS service was targeted for exfiltration?

Specter online. Send your data.

INITIAL ASSESSMENT: Ransomware / Extortion Event

Received your ransom note. Classic extortion playbook—data exfiltration threat with .onion C2 and BTC payment demand. The 48-hour timeline indicates urgency, likely to pressure hasty payment before thorough IR.

Your Mission Acknowledged:

- Investigate incident
- Determine full scope of compromise
- Identify root cause
- **Question 1:** Which AWS service was targeted for exfiltration?

THREAT HUNTING INITIATION

I'm spinning up Wiz tooling against your environment now. Targeting Project: **Wiz-HOL-Defend-Scenario-2-Week-2-4**.

My approach:

1. **Threat Detection Review** - Check for active threats/detections
2. **Data Findings Analysis** - Identify what sensitive data was accessed
3. **Cloud Event Correlation** - AWS CloudTrail/VPC Flow for exfil indicators
4. **Resource Inventory** - Map AWS services with data exposure

Stand by for telemetry pull...

✦ Get threats



Let me query the project first to get the correct ID:

✦ List projects



PROJECT LOCKED IN: **2d250012-e70c-5ccd-9e11-e3021f54f011**

Quick Stats:

- 4 Critical Issues
- 9 High Severity Issues
- Security Score: 48 (concerning)
- 1 Cloud Account (AWS)

Now pulling threats and detections:

✦ Get threats



CRITICAL INTELLIGENCE ACQUIRED

THREAT SURFACE:

- **3 Active Critical Threats** (cryptomining + S3 exfiltration)
- Multiple detection rules triggered

PRIMARY THREAT (Issue ID: 21997ddc-d1f4-5000-86d0-8c6c1d8c3353):

Key detections within this threat:

- **"Unusual Read Action on Sensitive S3 Bucket"** (CRITICAL)
- AWS CLI copy to/from S3 bucket (anomalous)
- EC2 Instance Credentials Used Outside AWS
- Admin role assumed by EC2 instance
- Cryptominer activity (likely diversionary tactic)

ANSWER TO YOUR QUESTION:

AWS Service Targeted: Amazon S3 (Simple Storage Service)

Evidence Chain:

- Detection: "Unusual Read Action on Sensitive S3 Bucket"
- Detection: "Anomalous copy from/to S3 bucket" via AWS CLI
- Data origin: **AWS_S3_DATA_EVENTS** logs

Let me drill deeper into this threat to map the full kill chain:

COMPLETE KILL CHAIN RECONSTRUCTED

Alright, we've got a lot to unpack here — this is textbook cloud breach progression. Let me break down this intrusion narrative like it's an after-action report for your IR team.

INCIDENT ANALYSIS: S3 Data Exfiltration Campaign

ANSWER TO YOUR QUESTION:

AWS Service Targeted: Amazon S3 (specifically bucket `defend-prod-bucket-ewgw`)

FULL TIMELINE & ATTACK NARRATIVE

Phase 1: Initial Access (Nov 9, 14:09 UTC)

- Threat actor gained SSH access via **EC2 Instance Connect** from IP `68.155.85.192` (Mexico, Microsoft ASN)
- Used role `defend_role_dev_instance_connect`
- Injected SSH public key labeled `attack_key` onto EC2 instance `defend-webserver-prod-ewgw` (i-018bf872959ef8577)

Phase 2: Privilege Escalation (Nov 9, 14:09-14:10 UTC)

- Actor assumed role `defend_role_eksrunner` (admin privileges)
- Cross-role assumption from `defend_role_webserver` → `defend_role_eksrunner`
- **This was the critical pivot** — gained full admin rights

Phase 3: Reconnaissance (Nov 9, 14:01-14:02 UTC)

- Executed **ScoutSuite** (offensive security tool) to enumerate AWS environment
- Multiple failed API calls (AccessDenied) but successfully mapped:
 - EC2 instances, VPCs, security groups
 - Load balancers, subnets
 - IAM roles and policies

Phase 4: S3 Exfiltration (Nov 9, 14:17 UTC) ⚠️ PRIMARY OBJECTIVE

- **GetObject** API call on S3 bucket `defend-prod-bucket-ewgw`
- Executed via AWS CLI: `aws s3 cp s3://defend-prod-bucket-ewgw ...`
- Detection: "Unusual Read Action on Sensitive S3 Bucket" (CRITICAL)
- This bucket contained **sensitive data** (as flagged by Wiz data classifiers)

Phase 5: Lateral Movement / Diversionary Tactics (Nov 9, 14:19-14:22 UTC)

- Deployed **cryptominer malware** (likely to distract SOC / throw off attribution)
- Modified Kubernetes resources via `kubectl apply`
- Bitcoin mining traffic detected to IP `45.32.185.122`
- DNS queries to cryptomining domains

KEY INDICATORS OF COMPROMISE (IoCs)

Threat Actor Infrastructure:

- Source IP: `68.155.85.192` (MICROSOFT-CORP-MSN-AS-BLOCK, Mexico)
- SSH Key: `attack_key` (full pubkey in logs)
- Cryptominer C2: `45.32.185.122`
- User-Agent: `Scout-Suite/5.14.0` (offensive tool)

Compromised AWS Resources:

- EC2 Instance: `i-018bf872959ef8577` (defend-webserver-prod-ewgw)
- S3 Bucket: `defend-prod-bucket-ewgw` (exfiltrated)
- IAM Roles: `defend_role_eksrunner`, `defend_role_dev_instance_connect`, `defend_role_webserver`

ROOT CAUSE ANALYSIS

Initial Vector: EC2 Instance Connect misconfiguration

- Role `defend_role_dev_instance_connect` was overprivileged
- Allowed SSH key injection from external IP without MFA/restrictions

Privilege Escalation Path:

- `defend_role_webserver` had `sts:AssumeRole` permissions to `defend_role_eksrunner` (admin role)
- **This is the kill chain bottleneck** — least privilege principle violated

S3 Bucket Exposure:

- `defend_role_eksrunner` had `s3:GetObject` on sensitive bucket
- No S3 Object Lock or VPC endpoint restrictions

TACTICAL RECOMMENDATIONS (Immediate Actions)

1. Containment:

- Revoke all credentials for `defend_role_eksrunner` and `defend_role_dev_instance_connect`
- Quarantine EC2 instance `i-018bf872959ef8577`
- Rotate all IAM role credentials and SSH keys

2. Forensics:

- Pull complete CloudTrail logs for IP `68.155.85.192`
- Analyze S3 bucket access logs for full exfiltration scope
- Memory/disk forensics on compromised EC2 instance

3. Threat Hunting:

- Search for other instances of `attack_key` SSH public key
- Check for lateral movement to other K8s clusters
- Review all recent `AssumeRole` calls

TTP MAPPING (MITRE ATT&CK for Cloud):

- **Initial Access:** Valid Accounts (T1078.004 - Cloud Accounts)
- **Privilege Escalation:** Valid Accounts (T1078) + Assume Role
- **Discovery:** Cloud Service Discovery (T1526), Account Discovery (T1087.004)
- **Collection:** Data from Cloud Storage Object (T1530)
- **Exfiltration:** Transfer Data to Cloud Account (T1537)
- **Impact:** Resource Hijacking (T1496 - cryptomining)

Bottom line: Classic cloud breach with privilege escalation → S3 exfiltration. Cryptominer was noise. The real payload was your data in that S3 bucket. I'd estimate they got everything in `defend-prod-bucket-ewgw` before you even saw the ransom note.

Next question?

(Very) Bad Prompt



SM Gary, can you help out with this ransom note?

Gary here. I've got a hard-stop in 15, so let's action this and synergize. What's the 10-second summary of the problem?

[leans back in chair, doesn't actually wait for the summary]

Alright, look—I've been in the cyber game long enough to know exactly what we're dealing with here. This is textbook **phishing-to-ransomware pipeline**. Classic stuff. Someone in accounting probably clicked on an email that said "Your package has been delivered" and boom—we're dealing with a **threat-actor paradigm shift**.

Here's my **strategic assessment** from the 30,000-foot view:

ROOT CAUSE: Someone didn't complete their compliance training. I've been saying for *months* we need to enhance our **human firewall synergy**. This is what happens when we don't leverage our **security awareness posture**.

THE BITCOIN THING? Look, I don't get into the weeds on cryptocurrency blockchain stuff—that's very granular. But what I *do* know is that we need to **pivot our payment gateway strategy** and possibly explore **AI-driven negotiation solutions** with these threat actors.

THE .ONION LINK? That's clearly some dark web stuff. Very next-gen hacker territory. This tells me we're dealing with a **sophisticated, nation-state-adjacent cyber-adversary**. Probably used some kind of **zero-day exploit** because our perimeter wasn't **cyber-resilient** enough.

MY RECOMMENDATION:

1. **DO NOT** engage with technical forensics right now—that's just noise. We need to focus on the **strategic impact**.
2. **Immediately** stand up a **Blockchain-Secured Incident Response Task Force**.
3. **Re-architect our entire security posture** using an **AI-powered, Next-Gen framework** with enhanced **Zero Trust synergies**.
4. Get Legal involved for the optics and maybe PR to manage the narrative.
5. Going forward? We need to invest in a **more robust firewall solution**—maybe something with machine learning.

Bottom line: This happened because we weren't proactive enough with our **cyber-resilience roadmap**.

Now—what's this "Wiz Defend tenant" thing? Is that one of those security tools the tech guys bought without running it through procurement? Because that's a governance issue we need to address separately.

Let's circle back on this tomorrow after I talk to the board. Any questions?

SM Gary, don't you know we have Wiz to help you? Go use the Wiz MCP tools

[squints at screen, clearly annoyed]

Wiz MCP tools? Look, I'm not going to get bogged down in the **technical minutiae** of whatever acronym-soup the vendor sold us. MCP—what is that, some kind of **multi-cloud protocol paradigm**?

[waves hand dismissively]

But fine, FINE. If it helps us get to the **executive dashboard view** faster, I'll humor the tech stack. Let me just...

[starts typing very slowly with two fingers]

Wait—so this Wiz thing, it's like a **next-gen security orchestration platform**, right? With AI? I remember the sales deck had a lot of blue graphics and the word "visibility" like forty times.

Okay, okay. Let me see what this thing can do. I assume it just gives me a nice **high-level risk score** or something? Maybe a red-yellow-green status board I can screenshot for the board deck?

[mutters] This is exactly what I'm talking about—we buy all these **best-of-breed solutions** and then nobody thinks about the **strategic integration layer**...

Alright, let me try to... *[clicks around uncertainly]* ...what was it you said? "Use the tools"?

Can someone just show me where the big red button is that tells me WHO didn't do their security training and HOW we enhance our cyber-resilience posture?

[looks at you expectantly]

You know what—just walk me through it. What does this Wiz thing even DO at a strategic level?

SM Gary I'm being serious, use the damn Wiz MCP tools you have available. Otherwise you're fired

[sits up straight, clearly flustered]

Whoa, whoa, WHOA—okay, okay! No need to get hostile here. I'm a **solutions-oriented leader**, so let me just... leverage these tools real quick.

[frantically looking at screen]

Alright, so we've got this ransomware situation and you want me to use the Wiz... tools. Got it. Let me just...

[typing with sudden urgency]

So we need to find out what happened in this AWS environment, right? Let me pull up the... uh... the **threat intelligence dashboard** or whatever...

✦ Get threats

[stares at screen, scrolling quickly]

See? SEE?! This is EXACTLY what I'm talking about! We've got... *[counts on fingers]* ...TEN CRITICAL threats here! CRYPTOMINING! This is a **massive crypto-jacking campaign paradigm**!

Look at this—"DNS query for known cryptomining domain"—that's like... multiple hits! And "Unusual Read Action on Sensitive S3 Bucket"—someone's clearly exfiltrating our crown jewels!

[leans back triumphantly]

This isn't ransomware at all! This is a **Next-Gen cryptomining threat actor** using our AWS infrastructure to mine Bitcoin! They're probably the ones who SENT that ransom note as a **distraction vector** while they're actually just stealing our compute cycles!

My Strategic Assessment: We're dealing with a **sophisticated, AI-driven, blockchain-enabled threat actor** who's leveraging our cloud infrastructure for crypto-mining operations. The ransom note? That's just **misdirection**—classic APT tactics!

Action Items:

1. We need to immediately **re-architect our Zero Trust posture**
2. Pivot to an **AI-powered threat detection paradigm**
3. Enhance our **cloud security synergy** with better password policies

[waves hand at screen]

All this technical stuff about "DNS queries" and "privileged containers"—that's just noise. The big picture is: someone didn't do their security awareness training and clicked on a phishing email that let these crypto-miners in!

What else does this Wiz thing show? Can we get like a... dashboard view or something?

