
GENERAL:

First Seen Time and Date: 20/12/2024 03:04:12 +0500
Insight: *Phishing → Credential Abuse → AWS Privilege Misuse (Insight-16681 - Discovery with Execution and Initial Access)*

Associated Signals:

1. Proofpoint TAP - User Received Phishing Email
2. Phishing Link Then Proxy Allow
3. First Seen AWS API Call: ListBucket2024-12-20 from User
4. Spike in AWS API Call from User
5. Suspicious AWS Lambda Enumeration
6. AWS GuardDuty Alert - UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration

---

SEVERITY CLASSIFICATION:

Priority: P2

Reason: This incident is classified as **P2** because a user endpoint was successfully compromised through a phishing campaign, and the attacker is actively using valid credentials in AWS for reconnaissance (S3, Lambda). A high-severity GuardDuty alert confirms credential misuse from an unusual IP. However, there is **no confirmed destructive activity or large-scale data exfiltration yet**, which is why this is contained at P2 instead of P1.

SOURCE DETAILS:

Source IPs:

- 125.118.246.104 (Phishing host) – Geolocated to Ningbo, Zhejiang, China
- 72.229.28.104 (User device observed accessing phishing URL) – New York, US

Source Hostname: anderson-karen-laptop

TARGET DETAILS:

Target Username: karen.anderson
Target Email Address: karen.anderson@corporatedomain.local
Target Device IP: 72.229.28.104 (workstation)

ADDITIONAL INFORMATION:

- **Phishing URL:**
  http://console.aws.amazon.account83sfas2.app-region121.io/signin
  → Fake AWS login page, hosted under **app-region121.io**, not affiliated with AWS.
- **File Basename:** text.txt (delivered attachment with phishing email).
- Domain uses **HTTP instead of HTTPS**, meaning credentials could be transmitted in cleartext.

INCIDENT DETAILS:

Between **20/12/2024 03:04 and 20/12/2024 04:05**, the user **Karen Anderson** was compromised through a targeted phishing campaign.

1. At **03:04**, Karen received a phishing email with attachment text.txt, delivered via Proofpoint TAP.
2. The email contained a link to a fake AWS login page (http://console.aws.amazon.account83sfas2.app-region121.io/signin).
3. At **04:04**, Zscaler proxy logs confirmed outbound traffic from **anderson-karen-laptop (72.229.28.104)** to the phishing URL, suggesting credentials were submitted.
4. Immediately after, suspicious AWS API activity began from IP **125.118.246.104 (China)** using Karen's credentials:
   - **First-time S3 ListBucket API call**
   - **Spike in AWS API calls**, consistent with scripted activity
   - **Lambda function enumeration** indicating reconnaissance of compute resources
5. The activity triggered a **GuardDuty UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration** alert, confirming credential theft and misuse.

This chain of events demonstrates successful phishing → credential theft → AWS account reconnaissance.

REMEDIATION ACTIONS:

Immediate Containment:

- Revoke all AWS credentials for **karen.anderson** (access keys, session tokens, console password).
- Enforce MFA on the account before re-enabling.
- Terminate any suspicious AWS sessions and block traffic from **125.118.246.104**.
- Isolate the endpoint **anderson-karen-laptop** for forensic analysis (check for malware/stealers).

Forensic & Audit:

- Review **CloudTrail logs** for privilege escalation, persistence (role creation), or unauthorized data access.
- Audit **S3 and Lambda** for unauthorized modifications, exposures, or hidden persistence.
- Search for **additional users targeted** by similar phishing emails.

Security Enhancements:

- Block the phishing domain **app-region121.io** across DNS, proxy, and mail gateways.
- Enable **AWS GuardDuty + Security Hub continuous monitoring**.
- Educate the user on phishing awareness and reinforce reporting procedures.
- Rotate credentials for any downstream systems accessed by Karen's account.

Conclusion:

This is a **P2 (High Priority)** incident involving **phishing, credential compromise, and AWS reconnaissance**. The compromise has not escalated to confirmed destructive or large-scale data theft yet, but **active credential misuse is ongoing** and requires immediate containment and audit.
