# **KZM** Security Incident Report

### **Table of contents**

[Security Incident Report 1](#_crlgmap8ym05)

[Table of contents 1](#_u17i2fv460ug)

[Executive summary 2](#_c8wmvmx6j3to)

[Investigation 3](#_sgg8djay179y)

[Response and remediation 4](#_bgoc8vygd0dj)

[Containment and eradication measures 4](#_kyhxcqk3n5c5)

[Recovery measures 4](#_givq0r4a9hwr)

[Recommendations 5](#_5hqs6q8ystb1)

# **Executive summary**

KZM Retail experienced a major data breach that compromised sensitive customer information, including credit card data, usernames, and associated locations. The breach occurred due to vulnerabilities in the company’s cloud environment, specifically involving a virtual machine (VM), a cloud storage bucket, and firewall configurations. A compromised VM (cc-app-01) was found to have been configured with an open SSH and RDP port, allowing a malicious actor to establish a connection and escalate privileges by exploiting a weak service account with full API access. The attacker infected the VM with malware and gained access to sensitive data stored in BigQuery. Data exfiltration was achieved through a publicly accessible cloud storage bucket, which the attacker used to transfer customer credit card information. Immediate response efforts focused on identifying, containing, and remediating the vulnerabilities across the affected cloud infrastructure.

# **Investigation**

A comprehensive investigation was conducted to determine the nature and extent of the compromise. The following findings were identified:

1. **Malware infection**: Forensic analysis confirmed the presence of malware on the compromised VM. The specific type and variant of the malware were identified through in-depth analysis, providing insights into the attacker's techniques and potential motivations.

2. **Unauthorized access**: Evidence revealed that the attacker gained unauthorized access to the compromised VM by exploiting open RDP and SSH services. The access logs and network traffic analysis provided crucial insights into the attacker's entry point and their subsequent activities.

3. **Privilege escalation**: The forensic examination indicated that the attacker leveraged the compromised VM to escalate privileges and gain access to sensitive systems and resources. Through the exploitation of user and service account credentials, the attacker was able to move laterally within the network and target additional services; in particular gaining unauthorized access to BigQuery.

4. **Data exfiltration**: The forensic analysis confirmed the exfiltration of credit card information, including card numbers, usernames, and associated locations. The attacker utilized a storage bucket with public internet access to initiate and facilitate the exfiltration, exporting the compromised data for later remote retrieval.

The findings provide valuable insights into the attack, enabling the incident response team to understand the attack vector, the attacker's actions, and the compromised data. These findings will serve as crucial evidence for further investigations, remediation efforts, and future cybersecurity enhancements.

# 

# **Response and remediation**

To effectively remediate the incident, a series of actions were taken in alignment with industry best practices. The following outlines the containment, eradication, and recovery measures implemented:

**Containment and eradication measures:**

1. **Shutting Down Compromised VM:** The infected virtual machine cc-app-01 was immediately shut down to stop the attacker from maintaining their presence in the environment.
2. **Removing Public IP and Ports Access:** The VM was recreated without a public IP and had secure boot enabled, preventing unauthorized external access. SSH access was restricted to specific internal IP ranges.
3. **Revoking Public Access to Storage Bucket:** The public access control list (ACL) of the storage bucket was revoked, and uniform bucket-level access control was enforced to secure sensitive data.
4. **Deleting Insecure Firewall Rules:** Broad firewall rules allowing open access via SSH, RDP, and ICMP were removed, and new restricted rules were implemented.
5. **Eradicating Malware:** The VM was deleted, and all related malware and infected components were eradicated from the environment.

### **Recovery measures:**

* 1. **Creating a Secure VM from Snapshot:** A new VM (cc-app-02) was created using a snapshot taken prior to the malware infection. This VM was configured with enhanced security features such as Secure Boot and a private IP address.
  2. **Enabling Firewall Logging:** Firewall logging was enabled to monitor incoming and outgoing traffic, ensuring better visibility of future network activities.
  3. **Verifying Compliance:** The environment was scanned for compliance with PCI DSS 3.2.1 standards. All critical vulnerabilities were resolved, and compliance was restored.
  4. **Monitoring and Logging:** Real-time monitoring was enabled across the system to detect future anomalies, and logging was activated for key services to ensure timely alerts in case of suspicious activity.

By implementing these measures, the security team successfully mitigated the immediate risks, removed the attacker's presence, and restored affected systems to a secure and operational state.

# **Recommendations**

This incident provided valuable lessons that can inform future cybersecurity practices and help prevent similar incidents. The following are recommendations that we suggest be implemented to mitigate similar attacks from happening in the future:

1. **Strengthen Access Controls:** Implement multi-factor authentication (MFA) and stronger password policies to reduce the risk of brute-force attacks on cloud resources. This would ensure that unauthorized access through weak credentials is mitigated.
2. **Regular Security Audits:** Conduct regular audits of firewall rules, storage bucket permissions, and virtual machine configurations to ensure no misconfigurations exist. Automated tools should be used to check for open ports and publicly accessible resources.
3. **Improve Incident Response Procedures:** Enhance incident response plans by including more frequent and simulated breach drills. The team should be trained to quickly identify, contain, and respond to breaches with well-documented procedures to minimize damage.
4. **Encrypt Sensitive Data:** Ensure that sensitive customer information, such as credit card details, is encrypted both at rest and in transit. This would prevent data exfiltration from being easily achieved even if access is compromised.

These measures, if implemented, will help prevent similar breaches in the future and strengthen the company’s overall security posture.