Cymbal

Security Incident Report

Table of contents

***

This security incident report was written by Tim A. Fongern on March 29, 2025 as part of the capstone project for the Google Cloud Cybersecurity Certificate.

The underlying facts are fictitious.

***

Executive summary

Cymbal Retail experienced a significant security incident involving unauthorized access to its cloud environment. The breach resulted in the exposure of sensitive customer credit card information, including card numbers, usernames, and associated locations. The attack was facilitated by multiple security misconfigurations, including an insecure firewall, an exposed virtual machine (VM) with open SSH and RDP ports, and a publicly accessible storage bucket.

The security team detected unusual activity, which led to an internal investigation. The malicious actor gained initial access by exploiting open ports on the cc-app-01 VM, executed a brute-force attack, deployed malware, escalated privileges using a compromised service account key, and ultimately exfiltrated data from BigQuery via a publicly exposed storage bucket.

This report details the response and remediation actions taken, as well as recommendations to mitigate similar risks in the future.

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, user names, 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. **VM containment and removal**
   - The compromised VM (cc-app-01) was shut down and deleted.
   - A new VM (cc-app-02) was created from a trusted snapshot, using a private IP address and enabling secure boot.

2. **Credential revocation**
   - The compromised service account keys were revoked.
   - New, least-privileged access credentials were issued.

3. **Firewall adjustments**
   - SSH and RDP access were restricted to only internal IP ranges.
   - Firewall logging was enabled to monitor network access.

4. **Storage bucket security enhancement**
   - Public access to the storage bucket was removed.
   - Fine-grained access control was replaced with uniform bucket-level access permissions.

5. **Malware and threat removal**
   - Threat-hunting teams scanned for additional signs of malware.
   - The malicious domain associated with the attacker was blacklisted.

Recovery measures

1. **Restoration of services**
   - All affected cloud services were restored using secured configurations.
   - BigQuery was reviewed for additional unauthorized access.

2. **Security patching and configuration updates**
   - Security patches were applied to all cloud infrastructure components.
   - Default service account permissions were restricted.

3. **Forensic investigation & audit**
    - Full forensic analysis was conducted to determine the timeline of events.
    - Security audits were performed to identify and remediate any additional vulnerabilities.

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:

To mitigate similar risks in the future, Cymbal Retail should implement the following security best practices:

1. **Enforce least privilege access controls**
    1. Implement role-based access control (RBAC) to ensure that accounts only have the necessary permissions.
    2. Disable the use of default service accounts with full API access.

2. **Harden cloud resources and firewalls**
    1. Configure all VMs to use private IPs whenever possible.
    2. Restrict SSH and RDP access to internal, trusted networks.
    3. Enable firewall logging and regularly review access logs for anomalies.

3. **Implement continuous monitoring and threat detection**
    1. Deploy a Security Information and Event Management (SIEM) system for real-time monitoring.
    2. Enable anomaly detection alerts to identify unusual activities.

4. **Improve incident response and backup strategies**
    1. Conduct regular security drills and incident response exercises.
    2. Ensure proper encryption of sensitive data and maintain secured, isolated backups.

By implementing these measures, Cymbal Retail can significantly strengthen its cloud security posture and reduce the likelihood of future breaches.