Cymbal

Security Incident Report

Table of contents

Executive summary

Cymbal Retail experienced a significant security incident that compromised its cloud infrastructure, primarily through unauthorized access to a virtual machine (VM) hosted in the cloud environment. The breach originated when an attacker exploited exposed Remote Desktop Protocol (RDP) and Secure Shell (SSH) services on a cloud-based VM. Once inside, the malicious actor deployed malware and escalated privileges, and gained access to sensitive internal systems. The attacker was then able to exfiltrate customer credit card data by using a publicly accessible storage bucket.

The forensic investigation revealed multiple vulnerabilities, including misconfigured firewall rules, inadequate access controls, and a lack of network segmentation. The malware used by the attacker was specifically tailored to facilitate lateral movement and maintain persistence within the network. The attacker gained unauthorized access to BigQuery and exported customer data containing names, card numbers, and locations, which were later retrieved through remote means.

The cloud resources affected included the compromised VM instance, BigQuery datasets containing sensitive customer data, and an unsecured Google Cloud Storage (GSC) bucket that enabled data exfiltration. Prompt Incident response efforts led to the successful containment and eradication of the threat, the recovery of affected systems, and the implementation of strengthened security measures to mitigate future incidents.

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 future investigations, remediation efforts, and enhanced cybersecurity measures.

Response and remediation

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

Containment and eradication measures

.

1. The compromised VM was immediately isolated from the network to prevent further malicious activity and lateral movement.
2. All external RDP and SSH access was disabled on affected cloud resources to cut off the attackers' access points.
3. Malware was removed from the affected VM after conducting a full forensic scan to identify and clean infected files.
4. Firewall rules were reviewed and updated to restrict inbound and outbound traffic to only trusted IPs and necessary ports.
5. IAM roles and permissions were audited, and excessive privileges were revoked or minimized to reduce the blast radius of future compromises.

Recovery measures

1. The infected VM was reimaged using a clean, verified image to ensure no remnants of the malware remained.
2. Data backups were restored to replace any potentially compromised datasets in BigQuery and other affected services.
3. Service account credentials were rotated, and compromised credentials were disabled or deleted.
4. Logging and monitoring tools were enhanced to increase visibility into future suspicious activities, including audit logging and alerting for sensitive operations.

5. Security controls were reviewed and reinforced, including encryption of sensitive data and tighter access to public storage buckets.

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. Implement Zero Trust principles across all cloud environments. This includes strong identity verification, least-privilege access polices, and continuous monitoring of user and device behavior
2. Harden cloud configurations by conducting regular security posture assessments. This may include automatic checks for open ports, misconfigured firewall rules, and public access to sensitive resources.

3. Enhance incident response training and **playbooks** for the security team to ensure a quicker and more coordinated response in future incidents, especially for cloud-based attacks.
4. Deploy data loss prevention (DLP) tools and enforce encryption for data at rest and in transit to mitigate the risk of future data exfiltration attempts.