Cymbal

Security Incident Report

Table of contents

1. Executive summary

A significant data breach occurred at Cymbal Retail's cloud environment, resulting in the exposure of credit card information, including card numbers, user names, and associated locations, for a substantial number of users. The breach was detected by the security team after observing unusual activity within the cloud environment. The incident involved the exploitation of vulnerabilities in multiple cloud resources, including an insecurely configured firewall, storage bucket, and virtual machine. The attacker gained unauthorized access, escalated privileges, and exfiltrated sensitive data through a series of sophisticated steps

2. 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.

3. 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:

[Provide details about the remediation actions taken in response to the security incident. Include specific containment and eradication, and recovery actions.]

3.1 Containment and eradication measures

1. The infected VM cc-app-01 was shut down and deleted to prevent further unauthorized access and potential spread of the malware
2. Public access to the compromised storage bucket was removed to prevent unauthorized data access
3. Firewall rules were adjusted to restrict SSH access to only the internal IP range (35.235.240.0/20

3.2 Recovery measures

1. A new VM, named cc-app-02, was created from a known and trusted snapshot, configured to use a private IP address, and enabled with secure boot
2. Fine-grained access to the storage bucket was replaced with uniform bucket-level access control to ensure uniform access to all objects in the bucket by bucket-level permissions
3. Firewall logging was enabled to allow for better auditing of network access

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.

4. 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 strict access controls: Regularly review and update access permissions for all cloud resources, ensuring the principle of least privilege is applied. Avoid using default service accounts and implement strong authentication mechanisms, including multi-factor authentication
2. Enhance network security: Regularly audit and update firewall rules to restrict unnecessary open ports. Implement network segmentation to limit lateral movement in case of a breach. Enable logging for all critical systems and regularly review these logs for any suspicious activities.
3. Improve data protection: Implement encryption for all sensitive data, both at rest and in transit. Regularly review and update data retention policies, and ensure that sensitive information is not stored in publicly accessible locations
4. Conduct regular security assessments: Perform frequent vulnerability scans and penetration testing to identify and address potential security weaknesses in the cloud environment. This should include reviewing configurations of VMs, storage buckets, and other cloud resources