Cymbal

Security Incident Report

Table of contents

Executive summary

The security team detected unusual activity within the cloud systems, which led to the discovery of a significant security breach affecting the company's applications, networks, systems, and data repositories. Attackers had gained unauthorized access to sensitive customer information, including credit card data and personal details.

The breach involved malware infecting one of the application VMs. This VM had SSH and RDP services enabled and was assigned a public IP address, which allowed the attacker to connect through these ports.

It was found that the VM instance was created with a default service account that had full access to cloud APIs. This configuration, along with potentially excessive IAM roles granted to users accessing the instance, created a risk of privilege escalation.

The attacker used the compromised VM to access the service account's managed user key, which facilitated further escalation and targeting of additional services. Specifically, the attacker used the compromised credentials to exfiltrate unencrypted credit card information.

During the attack, the perpetrators also discovered a storage bucket with public access enabled from the internet. This bucket had fine-grained access control, allowing both IAM and ACLs at the bucket and individual object levels.

.

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. **Isolate of compromised VM**: The compromised VM cc-app-01 was immediately isolated from the network to prevent further unauthorized access and limit its impact on other systems.
2. **Restrict RDP and SSH access**: Firewall rules were promptly updated to restrict RDP and SSH access to the compromised VM, minimizing the potential for further exploitation through these services.
3. **Remove public storage bucket**: Public access to the storage bucket was removed and permissions for the bucket were changed to uniform bucket-level access.

Recovery measures

1. **Restore from trusted snapshot**: The compromised VM was restored from a trusted snapshot taken prior to the incident, ensuring a clean and secure state.
2. **Review security configuration**: A comprehensive review of security configurations was conducted across systems—including VMs, storage buckets, and network infrastructure—to identify and rectify any misconfigurations or weaknesses.
3. **Improve monitoring**: Monitoring mechanisms were strengthened, including the implementation of real-time log analysis to enable prompt identification of any future unauthorized access attempts or suspicious activities.

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. Conduct regular risk assessments: Perform periodic risk assessments to identify and prioritize potential security risks and vulnerabilities specific to your organization. This includes assessing systems, networks, applications, and data assets.

2. Implement multi-factor authentication (MFA): Enable MFA for all critical systems and accounts to add an extra layer of security. This measure helps protect against unauthorized access, even if passwords are compromised.

3. Implement the principle least privilege: Follow the principle of least privilege, granting users only the permissions necessary to perform their job functions. Regularly review user privileges and remove unnecessary access rights.

4. Conduct penetration testing: Regularly perform penetration testing and vulnerability assessments to identify and address security weaknesses. This measure helps uncover vulnerabilities before malicious actors exploit them.