# 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**

The security team noticed suspicious activity within the cloud systems. A deeper investigation into this activity quickly revealed that the company experienced a significant security breach affecting its applications, networks, systems, and data repositories. Attackers gained unauthorized access to sensitive customer information, including credit card details and personal data.

The incident involved malware infecting one of the application virtual machines (VMs). This compromised VM had SSH and RDP services enabled, along with a public IP address that permitted the attacker to connect through those ports.

It was found that the VM instance was created using the default service account, which had unrestricted access to cloud APIs. This setup, combined with possibly excessive IAM roles assigned to users accessing the instance, created a risk for privilege escalation.

As a result, the attacker exploited the compromised machine to access the managed user key associated with the service account. This allowed them to escalate the attack further and target additional services. In particular, the attacker used the compromised user credentials to exfiltrate unencrypted credit card information.

Throughout the attack, the perpetrators discovered a publicly accessible storage bucket on the internet. Furthermore, the bucket had fine-grained access controls, enabling the use of 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. **Isolation of the Compromised VM:** The compromised VM, cc-app-01, was swiftly isolated from the network to prevent any further unauthorized access and to mitigate its impact on other systems.
2. **Restriction of RDP and SSH Access:** Firewall rules were quickly updated to limit RDP and SSH access to the compromised VM, reducing the potential for further exploitation through these services.
3. **Removal of Public Storage Bucket:** Public access to the storage bucket was revoked, and permissions were adjusted to implement uniform bucket-level access.

### **Recovery measures**

1. **Restoration from Trusted Snapshot:** The compromised VM was restored from a reliable snapshot created before the incident, ensuring it returned to a clean and secure state.
2. **Review of Security Configuration:** A thorough review of security configurations was performed across all systems—encompassing VMs, storage buckets, and network infrastructure—to identify and address any misconfigurations or vulnerabilities.
3. **Enhanced Monitoring:** Monitoring capabilities were improved, including the implementation of real-time log analysis to facilitate the quick detection 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:** Regularly check for potential security risks and vulnerabilities in your organization’s systems, networks, applications, and data.
2. **Implement Multi-Factor Authentication (MFA):** Use MFA for all important systems and accounts to add an extra layer of security, making it harder for unauthorized users to gain access, even if passwords are stolen.
3. **Follow the Principle of Least Privilege:** Give users only the permissions they need to do their jobs. Regularly review user access and remove any unnecessary rights.
4. **Conduct Penetration Testing:** Perform regular penetration tests and vulnerability assessments to find and fix security weaknesses before attackers can take advantage of them.