CYMBAL SECURITY INCIDENT REPORT

Table of Contents

Security Incident Report 1
Table of contents 1
Executive summary 2
Investigation 3
Response and remediation 4
Containment and eradication measures 4
Recovery measures 4
Recommendations 5
My Assessment 5

Executive Summary

The Cymbal Security team recently discovered a security breach within the cloud environment affecting multiple cloud resources. A virtual machine and storage bucket were accessed and the malicious attacker was able to install malware, escalate their privilege and access the service account contained within the VM.

The attacker was able to obtain sensitive information including credit card numbers, user names, and the associated locations. The current time of the attack is currently unknown, but is being investigated.

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 Recovery

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. After reviewing the logs the corrupted VM instance was stopped and deleted.
2. The bucket access control was changed to a uniform control.
3. New firewall rules were implemented to prevent access to ports.

Recovery measures

1. A VM snapshot from a verified backup was used to create a second VM instance with correct firewall rules.
2. The storage bucket received access controls to prevent unauthorized 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.

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 lease privilege and Multi-Factor Authentication
2. Continuous monitoring & testing
3. Conduct risk assessment

MY ASSESSMENT:

After completing the lab, this incident report, and reviewing the Google Exemplar of this report activity there are various pieces of information that I could have included in this report. First, in the executive summary I could have expanded on the security breach information, provided specific details about the attacker as well as the attack, what was effected and the next steps.

In the response and remediation session, I could have separated the remediation methods and expanded in a brief 2-3 sentences on the implementation process.

In the recommendations section, I initially thought it meant recommendations related to the specific attack, however with lessons learned the value comes from looking at the big picture and how to implement changes in the future. Rather than focusing on the attack, it is important to look at the overall system on where changes can be made. Risk assessments, implementing multi-factor authentication, and least privilege, etc. are not specific to the attack, but necessary for the system as a whole.