Cymbal

Security Incident Report

Table of contents

Executive summary

The security team detected unusual activity within the cloud environment. The security team promptly investigated the incident, collected information, and analyzed log data to determine the breach's scope and impact.

A breach occurred, resulting in the exposure of SPII(sensitive private identifiable information) and PII(private identifiable information) for a substantial number of users, including credit card data and personal details.
The incident included a VM that was infected by malware. The VM was initially compromised due to SSH and RDP open ports.

The VM had excessive privileges that enabled that attacker to exploit it and gain privileged access to other services. This service was used later to draw sensitive information from our cloud environment.

The security team at Cymbal Retail was unable to attribute the perpetrator of the data breach and is still undergoing forensic analysis to determine its exact times.

To exfiltrate the data out of the system, the attacker used a publicly accessible storage bucket with public internet access enabled.

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:

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

Containment and eradication measures

1. **Isolation of infected resources:** The infected VM cc-app-01 was shut down and deleted.
2. **Restrict external access:** Public access to the storage bucket was removed and fine-grained access was replaced with uniform bucket-level access control.
3. **Restrict RDP and SSH access:** The firewall rules were adjusted to restrict SSH access to only the internal IP range 35.235.240.0/20.

Recovery measures

1. **Restoration from a trusted source:** A new VM, named cc-app-02, was created from a known and trusted snapshot.
2. **Eradicate any other misconfiguration:** The VM is configured to use a private IP address, and enabled with secure boot to prevent similar issues in the future.
3. **improved auditing and monitoring:** Firewall logging was enabled.

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. To ensure a secure cloud environment, we recommend to follow the **principle of least privilege**. By following this rule, we will remove any unnecessary access to our cloud environments. This includes assessing systems, networks, applications, and data assets.
2. By implementing **multi-factor authentication**, we can make sure that any system in our cloud environment has another layer of security.
3. By regularly carrying out **penetration testing**, we can make sure that we will notice any vulnerability, and fix it before anyone with bad intentions will exploit them.