Phishing Incident Investigation 2024-12-18 #5

Globe Sistemas - Av. Libertador Jardin America

FINAL REPORT OF THE PHISHING INCIDENT

Executive summary

On December 28, 2022, at 7:20 p.m. Pacific Time, the organization experienced a security incident during which an individual was able to gain unauthorized access to customers' personally identifiable information (PII) and financial information.

Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential lost revenue. The incident is now closed and a thorough investigation has been conducted.

Chronology

At approximately 3:13 p.m. Pacific Time on December 22, 2022, an employee received an email from an external email address. The email sender claimed that they had successfully stolen customer data.

In exchange for not disclosing the data on public forums, the sender requested a cryptocurrency payment of $25,000. The employee assumed the email was spam and deleted it.

On December 28, 2022, the same employee received another email from the same sender. This email included a sample of the stolen customer data and a further payment demand of $50,000. That same day, the employee notified the security team, who began their investigation into the incident.

Between December 28 and December 31, 2022, the security team focused on determining how the data was stolen and the extent of the theft.

Investigation

The security team received the alert and went to the scene to begin the investigation.

The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.

After confirming the vulnerability of the web application, the security team analyzed the access logs of the web application. The logs indicated that the attacker accessed information from thousands of purchase confirmation pages.

Answer and solution

The organization worked with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident.

After the security team reviewed the associated web server logs, the cause of the attack was very clear. There was a single log source that showed an exceptionally high volume of customer orders listed sequentially.

Recommendations

To prevent future recurrences, we are taking the following measures: Performing routine vulnerability scans and penetration testing.

\*Implement the following access control mechanisms:

\*Implement whitelists to allow access to a specific set of URLs and automatically block all requests outside this URL range.

\*Ensure that only authenticated users have authorized access to content.