Incident Report

Initial report and findings

April 19, 2024

Incident date and time

Date: 4/18/24

Time: Approximately 4:08 PM EST to 5:16 PM EST

Incident summary

Terminal Profile Numbers (TPNs) were deactivated causing merchants to not be able to process transactions, due to a Bot attack. No sensitive information was compromised.

Summary of issue

A BOT attack using a compromised user login circumvented the user hierarchy check and deactivated some TPNs in the iPOSPays Gateway. No sensitive information was compromised nor was there any data lost due to this incident. The only impact to customers was the inability to run transactions for a brief period.

The credentials that were used for the attack were deleted approximately 30 minutes after first deactivation of the TPNs, stopping further deactivations. As an immediate measure all effective TPNs were restored, and transactions were able to be processed.

Once TPNs were restored to an active state, the end users were able to run transaction and close any transactions that were processed throughout the day

Corrective measurements have been implemented to prevent this from recurring.

Root cause analysis

Through the use of APIs the Bot attack was able to Delete TPNs.

Response handling

- At 4:08 PM EST we received complaints of merchant not being able to be process transactions.
- Approximately at 4:40 PM EST User ID that was used was deleted.
- TPNs that were deactivated were restored at approximately 5:16 PM EST.

Remedial steps

- Hierarchy Logic check was reengineered to prevent API from deleting TPNs.
- Implementing Captcha Verification for user login, which will prevent any login attempt from any other end points other than our portal.
- Implementing “Rate Check” (Velocity check) for all backend APIs.
- Blocked the IP pool of the VPN provider, to prevent further attacks from happening from this VPN provider.
- We are adding additional hierarchy checks for all delete and edit API as a top priority.
- Continue investigation and enhance security as needed.