

Link to aptio: [customer v7.drawio - draw.io (diagrams.net)](https://app.diagrams.net/)

Scenario: The customer is reviewing her account balance on the internet. In the background, GFH Bank is allowing here access by validating asymmetrically (utilizing both public key and private key). She is logging onto the bank’s HTTPS website. In the meantime, vulcanator is trying to infiltrate the system by denying the customer access to her account. Vulcanator introduced a botnet on the bank’s server while performing a distributed denial of service attack on the banks website.

While the DDOS is in place, vulcanator is also capturing trying to capture the customers data such as user name, password, bank login credentials, etc. by running a script kiddie to capture this information.

GFH Bank have in place a public key (for the customer) and private key (for the bank) to authenticate information being sent and received to validate the customers credentials.

In the meantime, the incident response team have detected anomalies in the event logs which triggered an alarm on the system.

Vulcanator credentials were invalid, as indicated in the event logs. GFH also have in place packet sniffers who detected an invalid ip address on the network.