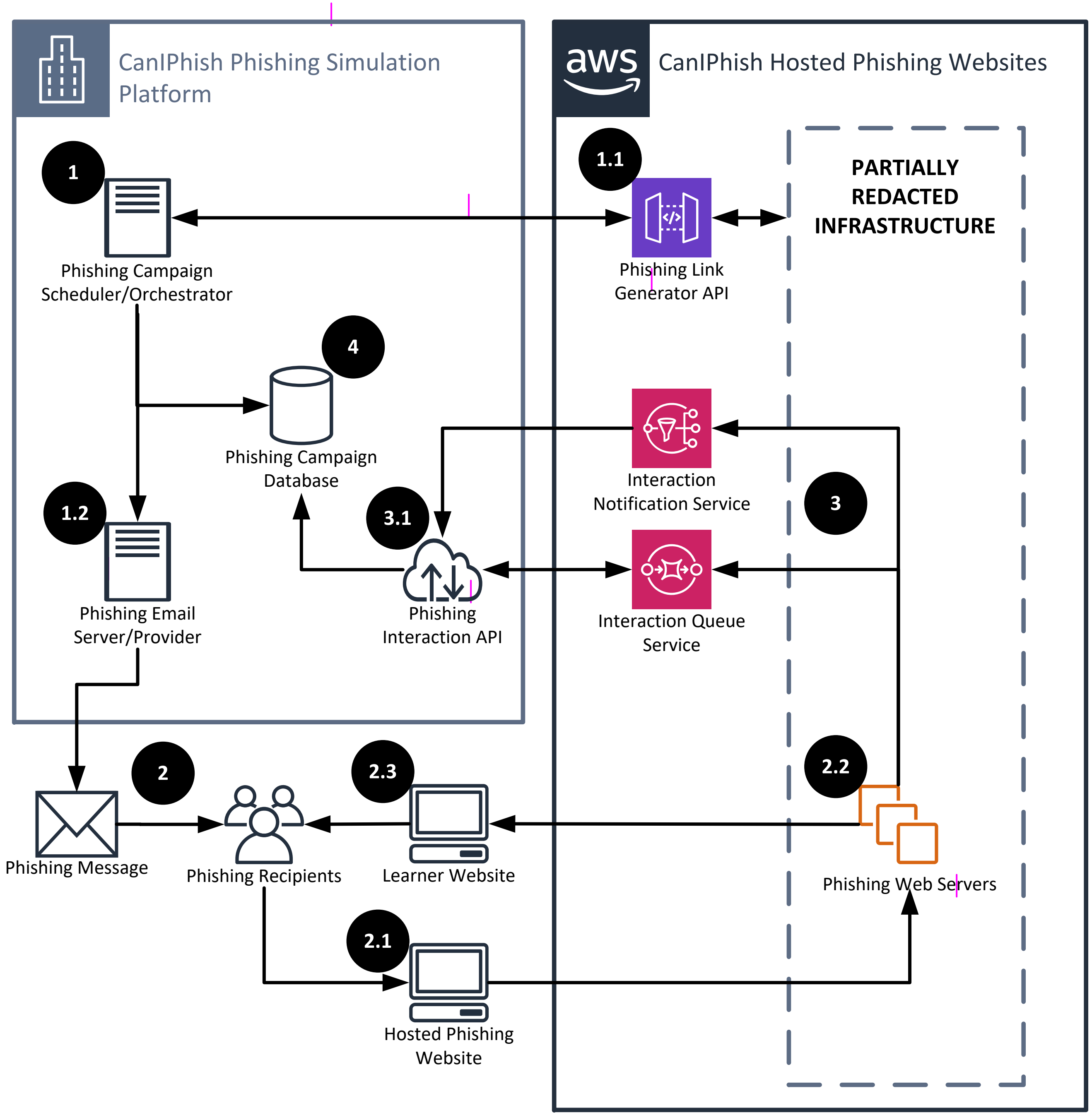
CanIPhish Phishing Simulation Platform
aws
CanIPhish Hosted Phishing Websites
1
Phishing Campaign Scheduler/Orchestrator
1.1
Phishing Link Generator API
PARTIALLY REDACTED INFRASTRUCTURE
4
Phishing Campaign Database
Interaction Notification Service
1.2
3.1
3
Phishing Email Server/Provider
Phishing Interaction API
Interaction Queue Service
2
2.3
2.2
Phishing Message
Phishing Recipients
Learner Website
Phishing Web Servers
2.1
Hosted Phishing Website

System Architecture Key

1. A phishing campaign is scheduled or begins delivery: The phishing orchestrator contacts the CanIPhish Phishing Link Generator to receive a unique phishing URL for each phishing recipient. This URL is then embedded into the phishing email each recipient will receive.

1.1: Phishing Link Generator API: Receives a number of unique identifiers to uniquely identify the third-party phishing simulator, campaign, recipient, phishing page, and action in the event of a compromise event (i.e. redirect to learner/education website)

Note: The campaign and recipient can be obfuscated or otherwise tokenized by the customer.

1.2: Phishing Email Server/Provider: Receives the phishing email from the campaign orchestrator and attempts delivery to the recipient mail server.

2. A phishing recipient receives the phishing message and clicks on the embedded phishing link.

2.1 Hosted Phishing Website: The recipient is presented with the intended phishing website which is automatically translated to one of 74 languages based on browser language preferences.

2.2 Phishing Web Servers: Captures recipient evidence (i.e. source IP address and embedded unique identifiers in the URL) and interactions such as page load, and password entry attempts *Note: No usernames, passwords or other entered data is captured. Simply the interaction is recorded.*

2.3 Learner Website: Depending on the action configured during link generation, the recipient may be redirected to a learner website.

3. Interactions are queued and/or notifications sent to the consumer/customer. Depending on the unique identifiers configured during link generation, a customer specific queue and/or notification service will receive information on the recent recipient interaction. The customer may choose to either receive the notification immediately or periodically poll the queue for new interaction information.

3.1 Phishing Interaction API: Unique identifiers configured during link generation will be provided to the API, along with interactions observed and any additional recipient evidence (i.e. source IP).

4. Phishing Campaign Database. Centralised customer/consumer database which records all campaign statistics.