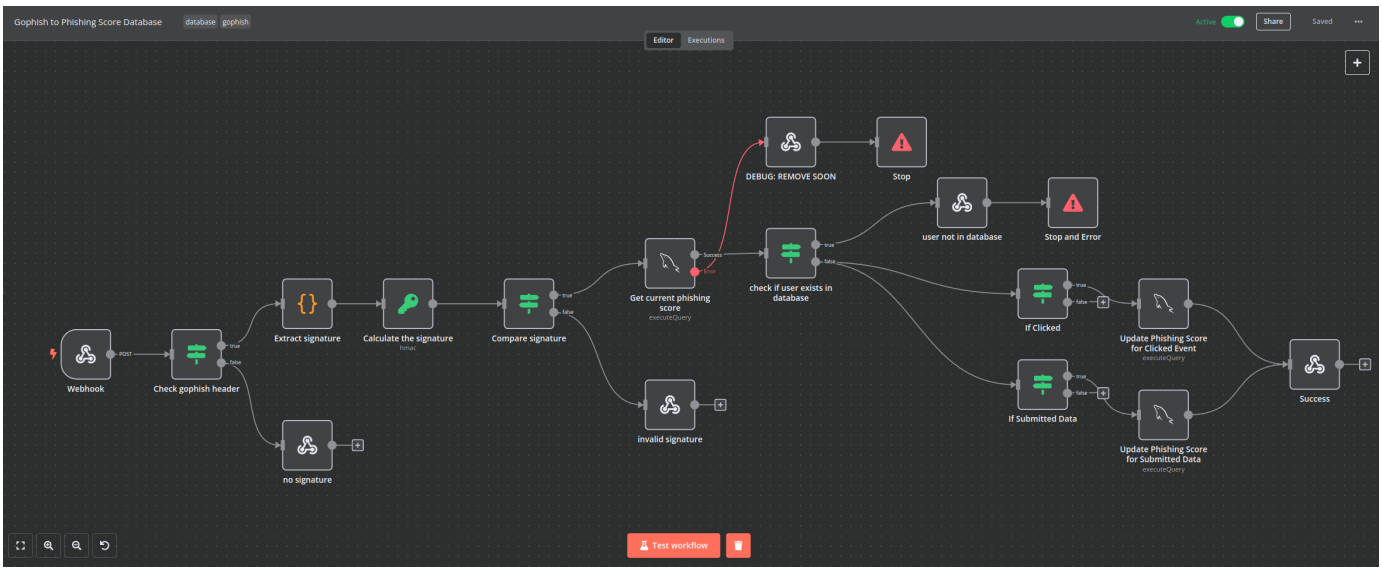
GoPhish Webhooks

How Gophish interacting with our inhouse automation plattform n8n with webhooks

Automating Phishing Score Analysis Using Gophish and n8n Workflows



In the realm of cybersecurity, automated workflows can significantly enhance the efficacy of phishing simulations and their subsequent analysis. Gophish, a popular open-source phishing toolkit, allows cybersecurity teams to conduct realistic phishing exercises to gauge the awareness and responses of their users. Integrating Gophish with n8n, a workflow automation tool, can streamline the process of scoring and tracking user interactions across multiple phishing campaigns. This integration is accomplished through Gophish's webhook system and n8n's capability to process and respond to incoming data in real time.

Overview of the n8n Workflow

The attached screenshot provides a detailed look at how phishing event data from Gophish is processed through an n8n workflow. Here's a breakdown of the key steps in this pipeline:

1. Webhook Reception: The n8n workflow starts with a webhook node configured to receive POST requests from Gophish. Each POST request includes detailed event data, such as the campaign ID, the recipient's email, and the type of action (e.g., link clicked).
2. Signature Verification: Security is paramount, so the workflow includes a step to check and verify the x-gophish-signature header. This signature is computed using a secret key known only to Gophish, ensuring that the data originates from a trusted source and has not been tampered with during transit.

Signature Processing

Extract Signature: The signature from the header is extracted.
Calculate Signature: The workflow recalculates the expected signature based on the received data and the secret key.
Compare Signature: The calculated signature is then compared against the received signature to confirm authenticity.

Database Interactions

4. User Validation: Checks if the user's email from the event is present in the database.
5. Phishing Score Update: Depending on the user's action, their phishing susceptibility score is updated. Actions like clicking a phishing link or submitting data through a phishing form negatively impact their score.
6. Debugging and Error Handling: Notably, there is a debug node labeled "DEBUG: REMOVE SOON" that aids in troubleshooting by providing error messages when things go awry. This node is temporary and will be removed once the workflow is fully operational and stable.
7. Conditional Logic: The workflow includes conditions to handle different scenarios, such as actions taken by the user (e.g., clicking a link or submitting data), and adjusts the phishing score accordingly.

Example HTTP POST Request from Gophish to n8n
Here is how an example POST request is structured when Gophish triggers a webhook due to a user action:

```
POST /webhook/d96af3a4-21bd-4bcb-bd34-37bfc67dfd1d HTTP/1.1
Host: 28efa8f7df.whiterabbit.htb
x-gophish-signature: sha256=cf4651463d8bc629b9b411c58480af5a9968ba05fca83efa03
Accept: */*
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Type: application/json
Content-Length: 81

{
  "campaign_id": 1,
  "email": "test@ex.com",
  "message": "Clicked Link"
}
```

We have attached a json file of a completed workflow where an invalid signature is provided
gophish_to_phishing_score_database.json

Security Mechanism: Signature Verification

The x-gophish-signature in each request plays a crucial role in ensuring the integrity and security of the data received by n8n. This HMAC (Hash-Based Message Authentication Code) signature is generated by hashing the body of the request along with a secret key. The workflow's verification of this signature ensures that the messages are not only intact but also are sent from an authorized source, significantly mitigating the risk of spoofed events for example SQLi attempts.

Conclusion

Integrating Gophish with n8n via webhooks offers a robust solution for automating the management of phishing training campaigns and user scoring. This setup not only saves time and reduces errors by automating repetitive tasks but also strengthens the overall cybersecurity posture by providing timely and accurate analysis of user behavior in phishing simulations. As phishing threats evolve, such integrations will be crucial in helping organizations stay ahead of potential security breaches.