

Comprehensive Report on Setting up a Phishing Campaign Using Gophish

Group 5:

1. Ivan Kasvan Opio
 2. Austine Baraka
 3. Barnice Wakiro Njoroge
 4. Murungi Micheal Charles
 5. Emmanuel Kofi Ansah-Anobah
 6. Kitso Bantom
-

1. Introduction to Phishing Campaigns

Phishing campaigns are a prevalent method used by cybercriminals to deceive individuals and organizations into providing sensitive information, such as usernames, passwords, and financial details. This method leverages email spoofing and fake websites to lure victims into believing they are interacting with legitimate entities. Cybercriminals can use this stolen information to access sensitive systems, steal funds, or even impersonate individuals for further attacks.

This report focused on the process of setting up a phishing campaign using **Gophish**, an open-source phishing framework. The setup demonstrated in this report used DigitalOcean, a cloud service provider, to host the phishing server.

2. The Lab setup

Gophish has a powerful, free, open-source nature, which simplified the process of creating and executing phishing campaigns. It provided a user-friendly interface to manage email templates, track engagement (such as clicks and form submissions), and customize landing pages for different campaigns.

DigitalOcean was chosen for hosting the Gophish server for several reasons:

- **Ease of Setup:** DigitalOcean offered pre-configured cloud infrastructure, allowing quick deployment of virtual machines, which reduced the overhead of managing on-premise hardware.
- **Accessibility:** Hosting on a cloud platform like DigitalOcean ensured that the phishing server was accessible to users on the public internet without complex networking configurations.
- **Affordability:** DigitalOcean provided low-cost hosting options, making it an economical choice for cybersecurity testing environments.

- **Scalability:** As the phishing campaigns grew, or if more resources were required, DigitalOcean made it easy to scale up server capacity without downtime.

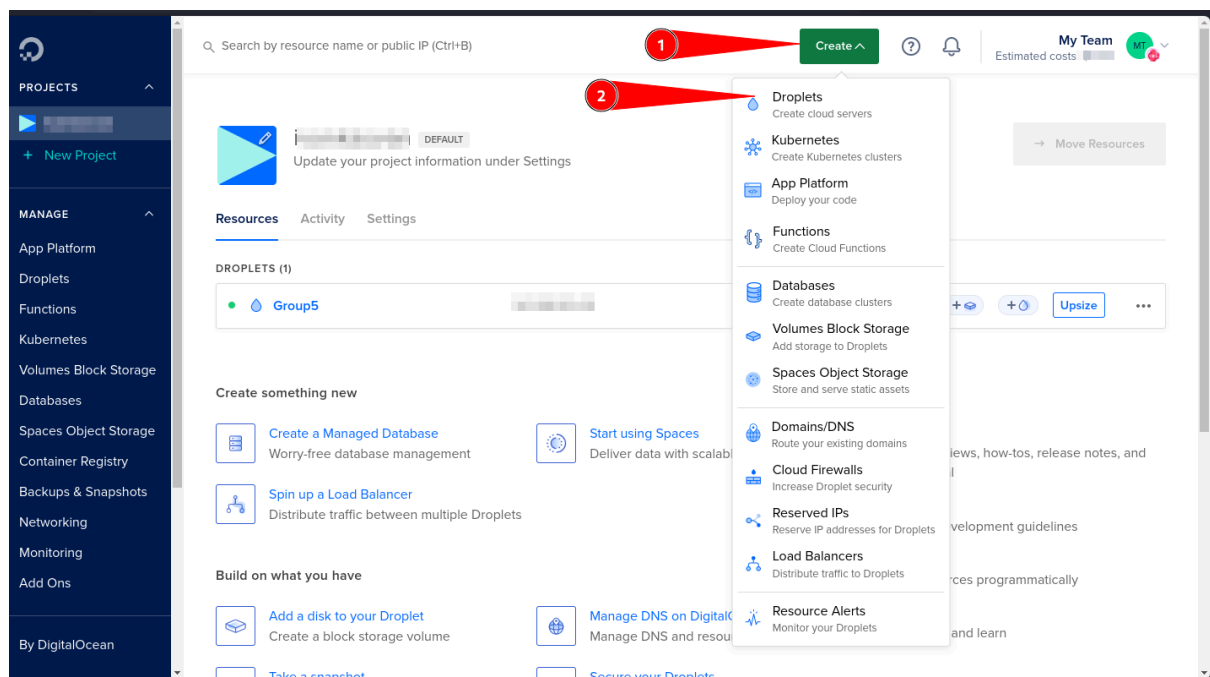
3. Setting Up a Phishing Campaign Using Gophish

3.1 Setting Up a Virtual Server on DigitalOcean

The group created a DigitalOcean account and then proceeded to set up a virtual machine (droplet) with Ubuntu as the operating system. A basic plan with 1GB RAM, 1 CPU, and 25GB SSD was selected. The group also set up a strong root password for the droplet and enabled monitoring for insights into performance.

Once the droplet was created, the group accessed it using an SSH client by logging into the server with the root user and password.

The screenshot below depicts the setup of Ubuntu server (Gophish hosting server):



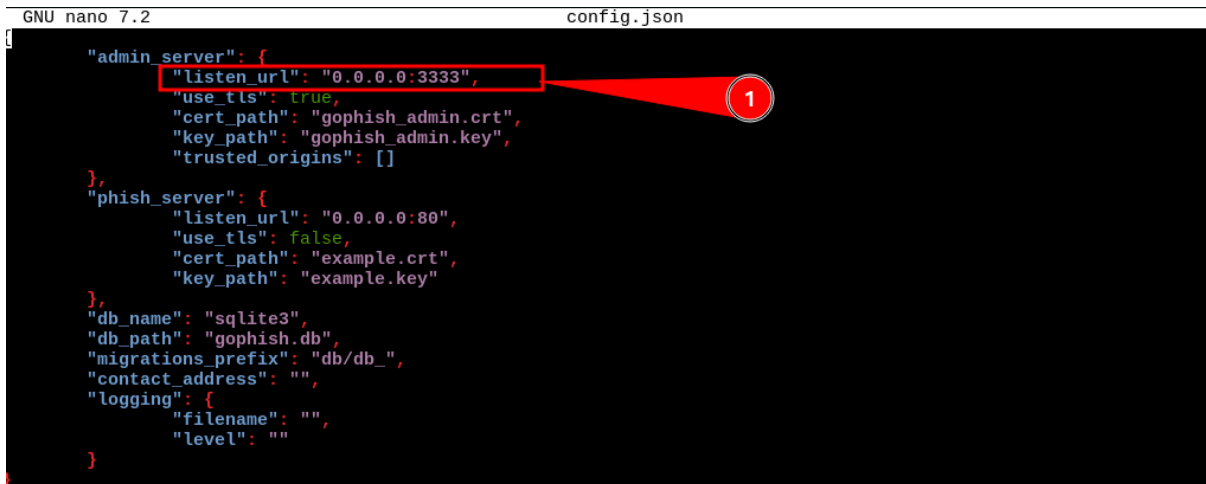
3.2 Installing Gophish on the Server

After logging into the server, the group downloaded the Gophish tool using the `wget` command. The downloaded Gophish package was then unzipped and configured. The configuration file, `config.json`, was modified to allow public access by changing the IP address to `0.0.0.0`.

Downloading Gophish onto the server:

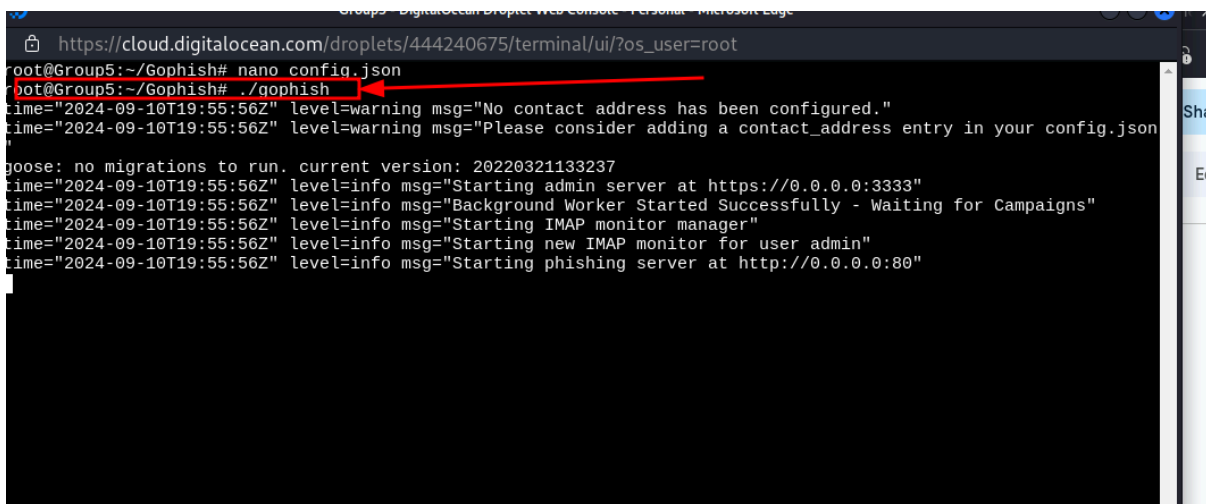
```
root@Group5:~#  
root@Group5:~# wget https://github.com/gophish/gophish/releases/download/v0.x.x/gophish-v0.x.x-linux-64bit.zip
```

Editing of the .json file



```
GNU nano 7.2 config.json  
  
  "admin_server": {  
    "listen_url": "0.0.0.0:3333",  
    "use_tls": true,  
    "cert_path": "gophish_admin.crt",  
    "key_path": "gophish_admin.key",  
    "trusted_origins": []  
  },  
  "phish_server": {  
    "listen_url": "0.0.0.0:80",  
    "use_tls": false,  
    "cert_path": "example.crt",  
    "key_path": "example.key"  
  },  
  "db_name": "sqlite3",  
  "db_path": "gophish.db",  
  "migrations_prefix": "db/db_",  
  "contact_address": "",  
  "logging": {  
    "filename": "",  
    "level": ""  
  }  
}
```

The Gophish server was then run using the command `./gophish`. The group received confirmation that the server was running on port 3333, and the default admin credentials were displayed.



```
https://cloud.digitalocean.com/droplets/444240675/terminal/ui/?os_user=root  
root@Group5:~/Gophish# nano config.json  
root@Group5:~/Gophish# ./gophish  
time="2024-09-10T19:55:56Z" level=warning msg="No contact address has been configured."  
time="2024-09-10T19:55:56Z" level=warning msg="Please consider adding a contact_address entry in your config.json"  
goose: no migrations to run, current version: 20220321133237  
time="2024-09-10T19:55:56Z" level=info msg="Starting admin server at https://0.0.0.0:3333"  
time="2024-09-10T19:55:56Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"  
time="2024-09-10T19:55:56Z" level=info msg="Starting IMAP monitor manager"  
time="2024-09-10T19:55:56Z" level=info msg="Starting new IMAP monitor for user admin"  
time="2024-09-10T19:55:56Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
```

4. Configuration of the Phishing Campaign in Gophish

4.1 Setting Up the Email Sending Profile

The group navigated to the Sending Profiles section in the Gophish dashboard and created a new profile. They filled in the necessary details, including the SMTP host, port, username, and password. They also tested the profile by sending a test email to verify the configuration.

Edit Sending Profile

×

Name:

G5_Campaign

Interface Type:

SMTP

SMTP From: ?

f[REDACTED]@gmail.com

Host:

smtp.gmail.com:465

Username:

[REDACTED]@gmail.com

Password:

☒ Ignore Certificate Errors ?

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

Show entries

Search:

Header ▲

Value ▼

4.2 Creating the Phishing Email Template

The group created a phishing email template by navigating to the Email Templates section. They provided a name for the template, crafted a subject line, and designed the email body using HTML to make it look like a legitimate notification from a well-known service provider.

Important: Suspicious Activity Detected on Your GFive Bank Account

Dear Customer,

We have detected unusual activity in your GFive Bank account. As a security precaution, we require you to verify your account immediately to prevent unauthorized access.

Please click the button below to log in and verify your details:

VERIFY NOW

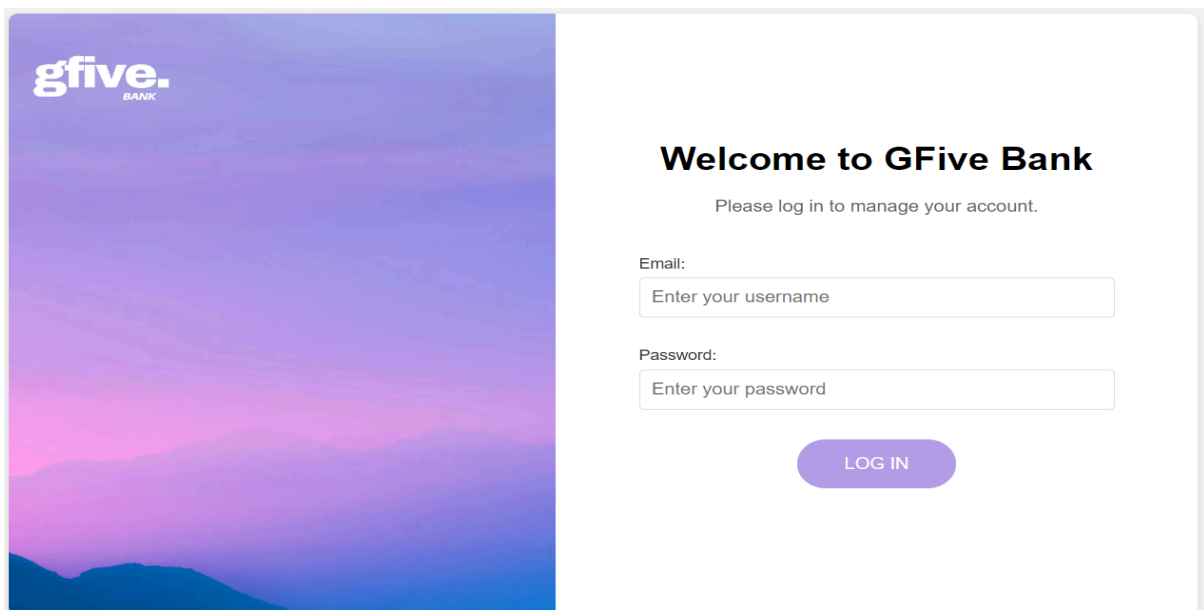
If you do not verify your account within 24 hours, your account access will be temporarily suspended.

Thank you for choosing GFive Bank.

© 2024 GFive Bank. All Rights Reserved.

4.3 Creating the Landing Page

The group created a landing page by navigating to the Landing Pages section in Gophish. They created a fake login page and enabled the feature to capture submitted data. A redirect to the legitimate website was also set up after the form was submitted to avoid suspicion from the user.



gfive.
BANK

Welcome to GFive Bank

Please log in to manage your account.

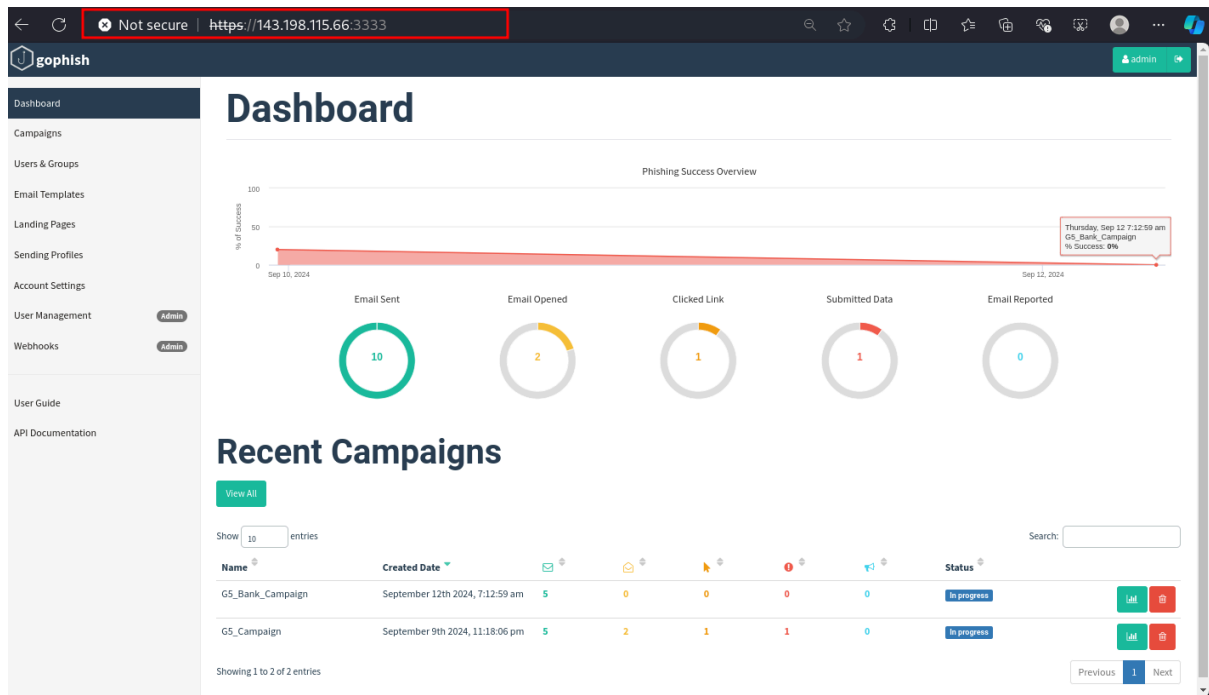
Email:

Password:

LOG IN

5. Launching the Phishing Campaign

The group created a user group by manually adding email addresses of the targets. Afterward, they created and launched the campaign by filling in the necessary details, including the email template, landing page, sending profile, and target group. They monitored the progress through the Gophish dashboard, tracking who opened the emails, clicked on the links, and submitted credentials.



Got Phished!!

