

Le serveur Gophish

L'objectif de cette procédure est d'expliquer la mise en place ,
l'installation et le paramétrage d'un serveur go phish

1 – Location d'une VM AWS

Dans un premier temps, il faut prendre une VM Windows server 2022 via Aws.
Le paramétrage est aussi possible avec une VM Linux, ici nous verrons sous OS
Microsoft.

Config minimum de la VM : 4Go de Ram.

1 – Installation de Go Phish

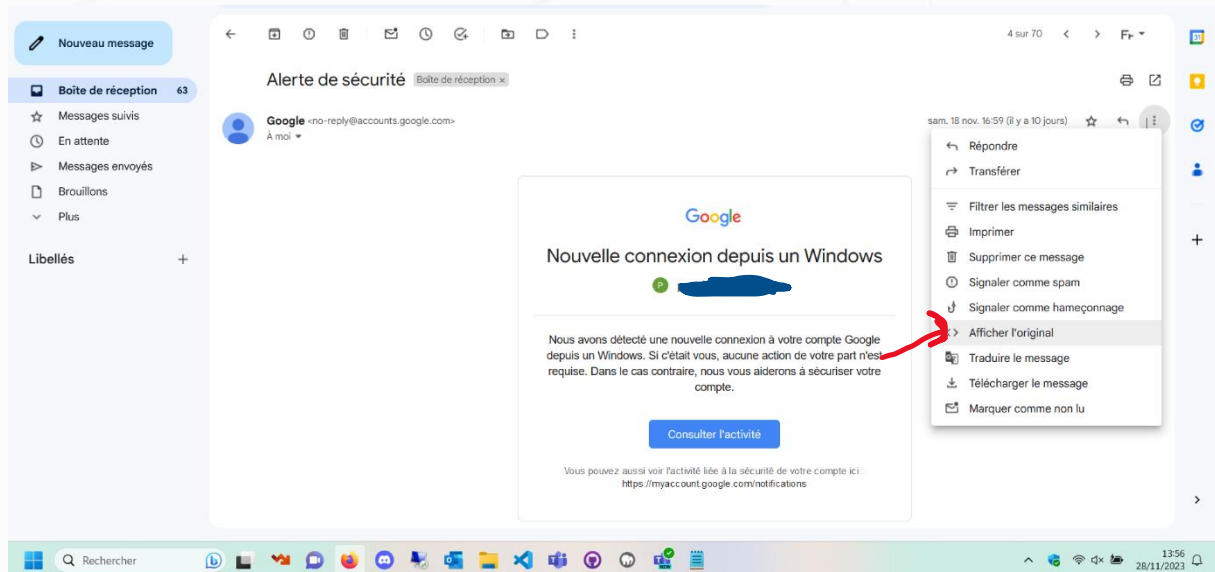
Tout d'abord, télécharger l'exécutable sur internet et le lancer sur le bureau de
la VM. Bien penser à ouvrir les ports **443 et 80** du pare-feu . Par défaut ,
l'adresse du server d'admin est sur localhost (127.0.0.1) . Pour le modifier,
chercher le fichier config.json dans le dossier ou Go phish a été installé puis
modifier les adresses IP en 0.0.0.0 :443 et 0.0.0.0 :80 (cf photo ci jointe)

```
{
  "admin_server": {
    "listen_url": "0.0.0.0:443",
    "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": ""
  }
}
```

1 – Paramétrage de Go Phish

Email Template :

Dans cette section il est possible de créer le template du mail via du code html. Plusieurs solutions sont possibles comme notamment récupérer le code source d'un mail via google mail (envoyer le template du mail sur une boîte google et explorer le contenu pour récupérer le code, ne marche qu'avec les boîtes mail Google). L'url du credential est ainsi renseigné automatiquement



Landing pages :

Il s'agit de la fausse page d'authentification vers laquelle l'utilisateur va être redirigé. Contrairement au template du mail, la page peut être faite en full html.

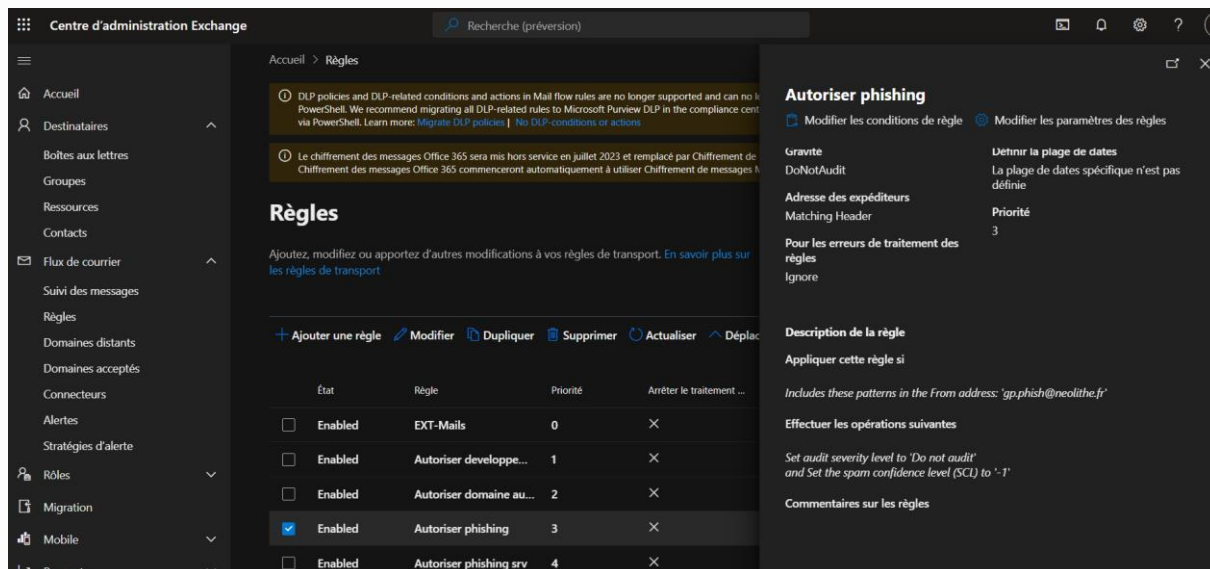
New campaign :

Pour lancer une nouvelle campagne, il faut choisir un template, une landing page et le groupe d'utilisateurs destinataires du phishing.

Pour l'url de retour des informations, il faut renseigner l'ip du serveur précédé de http (sans s).

Dans le portail 365, il faut autoriser l'adresse d'expéditeur à ne pas être bloquée par Defender. Pour cela il faut créer une règle dans Exchange Admin Center :

<https://admin.exchange.microsoft.com/>



Centre d'administration Exchange

Accueil > Règles

DLP policies and DLP-related conditions and actions in Mail flow rules are no longer supported and can no longer be managed via PowerShell. We recommend migrating all DLP-related rules to Microsoft Purview DLP in the compliance center via PowerShell. Learn more: [Migrate DLP policies](#) | No DLP conditions or actions

Le chiffrement des messages Office 365 sera mis hors service en juillet 2023 et remplacé par Chiffrement des messages Office 365 commenceront automatiquement à utiliser Chiffrement des messages Office 365

Règles

Ajoutez, modifiez ou apportez d'autres modifications à vos règles de transport. En savoir plus sur les règles de transport

+ Ajouter une règle Modifier Dupliquer Supprimer Actualiser Déplacer

État	Règle	Priorité	Arrêter le traitement...	
<input type="checkbox"/>	Enabled	EXT-Mails	0	X
<input type="checkbox"/>	Enabled	Autoriser développe...	1	X
<input type="checkbox"/>	Enabled	Autoriser domaine au...	2	X
<input checked="" type="checkbox"/>	Enabled	Autoriser phishing	3	X
<input type="checkbox"/>	Enabled	Autoriser phishing srv	4	X

Autoriser phishing

Modifier les conditions de règle Modifier les paramètres des règles

Garde

DoNotAudit

Adresse des expéditeurs

Matching Header

Pour les erreurs de traitement des règles

Ignore

Définir la plage de dates

La plage de dates spécifique n'est pas définie

Priorité

3

Description de la règle

Appliquer cette règle si

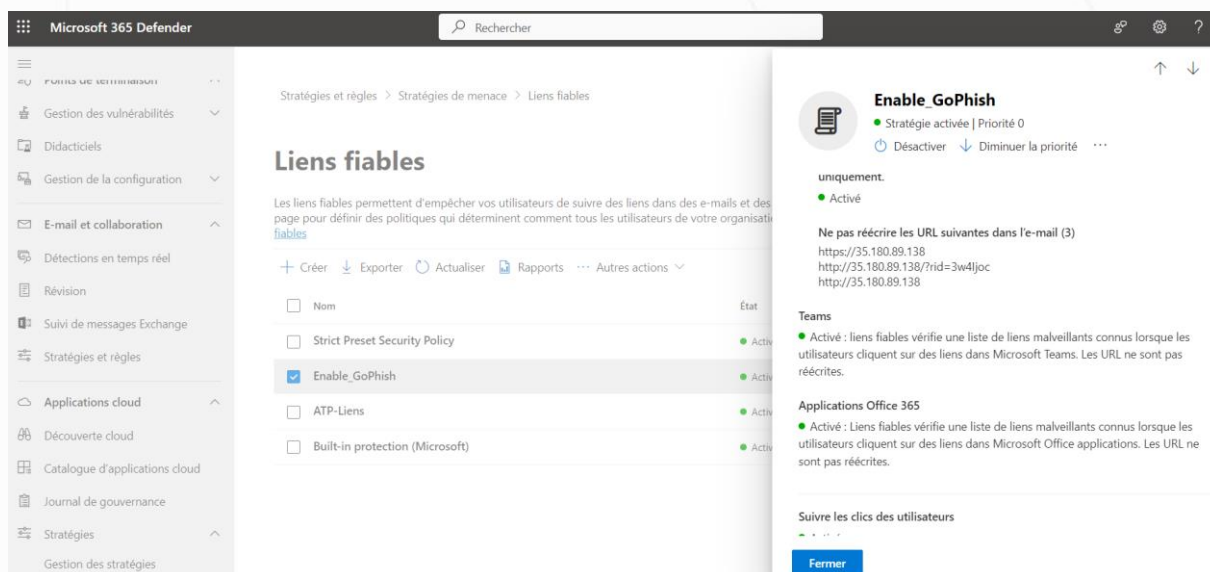
Includes these patterns in the From address: 'gp.phish@neolithe.fr'

Effectuer les opérations suivantes

Set audit severity level to 'Do not audit' and Set the spam confidence level (SCL) to '-1'

Commentaires sur les règles

Il faut également autoriser l'envoi des liens de phishing dans le mail en passant par le portail de sécurité Microsoft : <https://security.microsoft.com/>



Microsoft 365 Defender

Rechercher

Stratégies et règles > Stratégies de menace > Liens fiables

Liens fiables

Les liens fiables permettent d'empêcher vos utilisateurs de suivre des liens dans des e-mails et des pages pour définir des politiques qui déterminent comment tous les utilisateurs de votre organisation peuvent suivre des liens fiables

+ Créer Exporter Actualiser Rapports ... Autres actions

Nom	État
<input type="checkbox"/> Nom	
<input type="checkbox"/> Strict Preset Security Policy	Actif
<input checked="" type="checkbox"/> Enable_GoPhish	Actif
<input type="checkbox"/> ATP-Liens	Actif
<input type="checkbox"/> Built-in protection (Microsoft)	Actif

Enable_GoPhish

Stratégie activée | Priorité 0

Désactiver Diminuer la priorité

uniquement.

Actif

Ne pas réécrire les URL suivantes dans l'e-mail (3)

https://35.180.89.138
http://35.180.89.138/?rid=3w4ljoc
http://35.180.89.138

Teams

Actif : liens fiables vérifie une liste de liens malveillants connus lorsque les utilisateurs cliquent sur des liens dans Microsoft Teams. Les URL ne sont pas réécrites.

Applications Office 365

Actif : Liens fiables vérifie une liste de liens malveillants connus lorsque les utilisateurs cliquent sur des liens dans Microsoft Office applications. Les URL ne sont pas réécrites.

Suivre les clics des utilisateurs

Fermer

Reste à voir l'autorisation de l'adresse mail pour que Go Phish modifier l'expéditeur dans le header du mail