

Gophish钓鱼平台安装使用教程

一、钓鱼邮件概述

钓鱼邮件指利用伪装的电邮，欺骗收件人将账号、口令等信息回复给指定的接收者；或引导收件人连接到特制的网页，这些网页通常会伪装成和真实网站一样，如银行或理财的网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等而被盗取。

二、Gophish部署

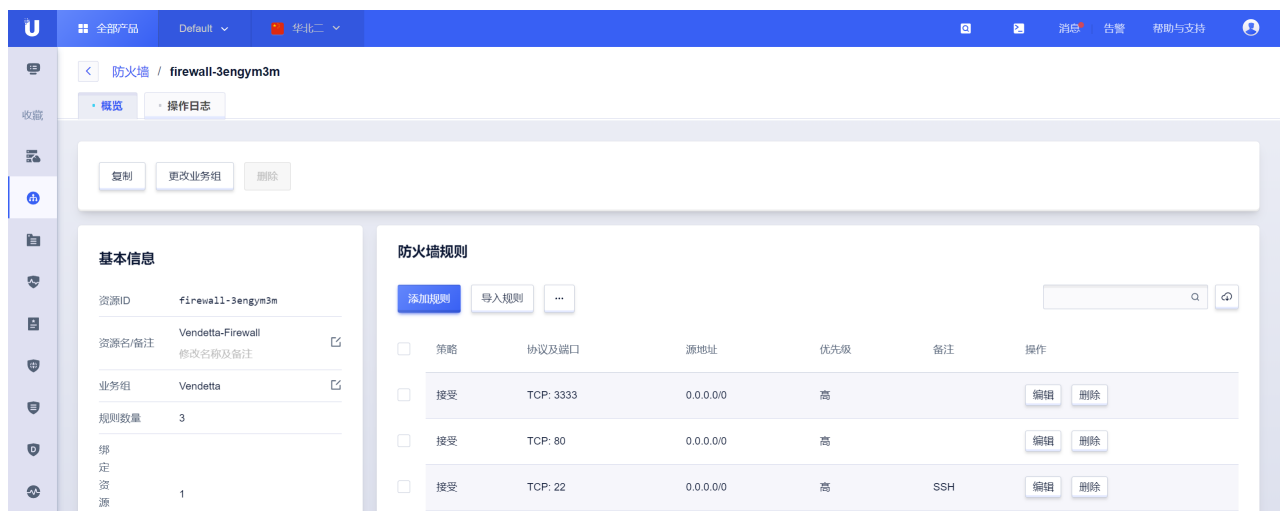


官方网站: <https://getgophish.com/>

软件下载: <https://github.com/gophish/gophish/releases>

部署环境: 云主机

底层系统: CentOS Linux release 8.3.2011



上传安装包并解压至安装目录: `unzip -d /opt/gophish gophish-v0.12.1-linux-64bit.zip`

修改配置文件: `vim /opt/gophish/config.json`

```
2      "admin_server": {
3          "listen_url": "0.0.0.0:3333",
4          "use_tls": true,
5          "cert_path": "gophish_admin.crt",
6          "key_path": "gophish_admin.key",
7          "trusted_origins": []
8      },
9      "phish_server": {
10         "listen_url": "0.0.0.0:80",
11         "use_tls": false,
12         "cert_path": "example.crt",
13         "key_path": "example.key"
14     },
15     "db_name": "sqlite3",
16     "db_path": "gophish.db",
17     "migrations_prefix": "db/db_",
18     "contact_address": "",
19     "logging": {
20         "filename": "",
21         "level": ""
22     }
23 }
```


脚本赋权：chmod +x gophish

服务启动：./gophish

启动后终端窗口会显示账号密码，复制登录后修改初始密码重新登录。

登录地址：<https://117.50.177.71:3333>

三、Gophish配置



Dashboard 平台概览

Campaigns 攻击配置

Users & Groups 受害者邮箱

Email Templates 邮件模板

Landing Pages 钓鱼网页

Sending Profiles 发件邮箱配置

Account Settings

User Management Admin

Webhooks Admin

User Guide

API Documentation

admin

Dashboard

No campaigns created yet. Let's create one!

3.1 Sending Profiles

Edit Sending Profile



Name:

163邮箱

Interface Type:

SMTP

SMTP From: ?

vendetta2023@163.com

Host:

smtp.163.com:465 邮箱服务器

Username:

vendetta2023@163.com 发件邮箱

Password:

..... 授权码

☒ Ignore Certificate Errors ?

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

Show 10 entries

Search:

Header

Value

X-Mailer

Vendetta 发件客户端



Showing 1 to 1 of 1 entries

Previous

1

Next

Send Test Email

发送测试邮件

Cancel

Save Profile

X-Mailer配置未配置的话邮件发送客户端显示是gophish

```
1 Received: from 192-168-111-32 (unknown [117.50.177.71])
2   by zwqz-smtp-mta-g4-2 (Coremail) with SMTP id _____wBH1nYy6yxk6oBrAg--.20279S2;
3   Wed, 05 Apr 2023 11:29:54 +0800 (CST)
4 Mime-Version: 1.0
5 Date: Wed, 05 Apr 2023 11:29:54 +0800
6 From: vendetta2023@163.com
7 X-Mailer: gophish
8 Subject: Default Email from Gophish
9 To: =?utf-8?q?=E5=BC=A0_?E4=B8=89?= <vendetta2023@163.com>
10 Content-Type: text/plain; charset=UTF-8
11 Content-Transfer-Encoding: quoted-printable
12 X-CM-TRANSID:_____wBH1nYy6yxk6oBrAg--.20279S2
13 Message-Id: <642CEB36.011EEB.00008@m12.mail.163.com>
14 X-Coremail-Antispam: 1Uf129KBjDUUn29KB7ZKAUJUUUUU529EdanIXcx71UUUUU7v73
15   VFW2AGmfu7bjvj3AaLaJ3UbIYCTnIWIEvJa73UjIFyTuYvj4RkwIgUUUUU
16 X-Originating-IP: [117.50.177.71]
17 X-CM-SenderInfo: xyhqvvhwddjiist6il2tof0z/xtbB0wtIKVXlyo-cdwABsm
18
19 It works!
20
21 This is an email letting you know that your gophish
22 configuration was successful.
23 Here are the details:
24
25 Who you sent from: vendetta2023@163.com
26
27 Who you sent to:=20
28   First Name: =E5=BC=A0
29   Last Name: =E4=B8=89
30   Position: =E6=B3=95=E5=A4=96=E7=8B=82=E5=BE=92
31
32 Now go send some phish!
```

邮件检测

概述 邮件头 邮件内容 URL分析 邮件附件 异常行为 威胁情报(IOCs) 自定义规则

主题: Default Email from Gophish

发件人名称(From): --

发件人地址(From): vendetta2023@163.com

实际发件人(Sender): --

收件人(To): 张三<vendetta2023@163.com>

抄送人(Cc): --

密送人(Bcc): --

回复地址(Reply): --

退信地址(Return): --

发送时间(Client): 2023-04-05 11:29:54 星期三

发送时间(Server): 2023-04-05 11:29:54 星期三

接收时间(Server): 2023-04-05 11:29:54 星期三

发件IP: [117.50.177.71] 中国-北京-北京

发件域名: 163.com

发件客户端: gophish

附件: --

邮件ID: <642CEB36.011EEB.00008@m12.mail.163.com>

被回复的邮件ID: --

邮件投递路径:

序号	时间	来自于	发送到	采用的协议
1	2023-04-05 11:29:54 星期三	192-168-111-32 (unknown [117.50.177.71])	zwqz-smtp-mta-g4-2 (Coremail)	SMTP

收件人数: 1

抄送人数: 0

密送人数: 0

邮件大小: 309B

Received减数: 1

恶意URL数/总量(正文): 0/0

恶意URL数/总量(附件): 0/0

恶意附件数/总量: 0/0


检测时间: 2023-04-05 11:35:56

方向: --

威胁级别: 信息

威胁标签: --

其他标签: 基本信息: 不包含链接 邮件头: 发件人一致 基本信息: 不包含附件 基本信息: Message-Id和from的后缀不一致 英文邮件



我们测试或者做钓鱼邮件的安全意识培训可以用公用邮箱，如果是真正的攻击，如果用公用邮箱，太容易辨识了。所以在确定受害者邮箱之后，通常会申请一个形似的邮箱域名，然后搭建邮箱服务器用于钓鱼邮件发送，提升真实性，提高上钩几率。

3.2 User&Groups

Edit Group

Name:

受害者

+ Bulk Import Users

Download CSV Template

下载CSV模板

First Nam

Last Nam

Email

Position

+ Add

Show

10

entries

Search:

First Name

Last Name

Email

Position

张

三

vendetta2023@...

法外狂徒

Showing 1 to 1 of 1 entries

Previous

1

Next

Close

Save changes

3.3 Landing Pags

















钓鱼页面是配合钓鱼邮件使用的，钓鱼邮件的最终目的，通常是通过钓鱼邮件来使受害者点击链接进入精心构造的钓鱼页面，通过钓鱼页面来诱导用户输入敏感信息，如密码等；或者通过钓鱼邮件诱导用户点击下载邮件附件，以此来向受害用户主机植入病毒或木马等。

一般情况下，钓鱼页面都是类似于**修改密码**或者**登录**之类的页面，并且要和钓鱼页面所模仿的页面做到尽可能的一样。


×



钓鱼网页测试

自动爬取静态页面

Source



B
I
S

 $\frac{1}{2}$
 $\frac{3}{4}$
 $\frac{5}{8}$
 $\frac{7}{8}$

Styles
 Format

推荐使用网站下载工具下载后导入

⚠ Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

<https://www.baidu.com>

用户在钓鱼页面提交信息后跳转的界面，建议配置为仿冒网站的真实界面。

Save Page

```
2 <head>
```

```
3  <title>钓鱼邮件测试</title>
4  </head>
5  <body>
6  <h1 align="center">钓鱼邮件测试</h1>
7
8  <form action="" method="post">
9  <table>
10 <tbody>
11     <tr>
12         <td>用户名: </td>
13         <td><input name="user" type="text" value="" /></td>
14         <td>密码: </td>
15         <td><input name="passwd" type="password" value="" /></td>
16         <td><input name="按钮名字" type="submit" valer="值" /></td>
17     </tr>
18 </tbody>
19 </table>
20 </form>
21 </body>
22 </html>
```

3.4 Email Templates

Edit Template



Name:

钓鱼邮件模板

 Import Email

导入email文件

Envelope Sender: ?

vendetta@qq.com 虚假的发送者，随意编辑。

Subject:

请重新登录修改您的密码!!!

Text

HTML



```
<html>
<head>
  <title></title>
</head>
<body>
<p>您好: </p>

<p>近期检测到您的账号口令存在异常登录, 请点击<a href="{{.URL}}">此链接</a>尽快修改密码, 谢谢配
```

这个链接会被自动替换为钓鱼网页的链接

☒ Add Tracking Image

 Add Files

import Email勾选了ChangeLinks to Point to LandingPage之后，邮件模板中的链接会被替换为钓鱼网站的链接，当目标点击邮件中的链接后，会跳转到后续在LandingPages里配置的钓鱼页面里。

```
1 <html>
2 <head>
3 <title></title>
```

```
4 </head>
5 <body>
6 <p>您好: </p>
7
8 <p>近期检测到您的账号口令存在异常登录, 请点击<a href="{{.URL}}">此链接</a>尽快修改密码, 谢谢配合! </p>
9 {{.Tracker}}</body>
10 </html>
```

邮件接收展示

[返回](#) [回复](#) [回复全部](#) [转发](#) [删除](#) [举报](#) [拒收](#) [标记为](#) [移动到](#) [更多](#)

请重新登录修改您的密码!!!

发件人: vendetta<vendetta@qq.com> (由 vendetta2023@163.com 代发, [帮助](#))

收件人: 张三<vendetta2023@163.com>

时间: 2023年04月05日 13:34 (星期三)

使用阿里云无影云桌面 4核8G低至1元/月 [立即抢购](#)

您好:

近期检测到您的账号口令存在异常登录, 请点击[此链接](#)尽快修改密码, 谢谢配合!

3.5 Campaigns

Launch Date && Send Emails By

Launch Date顾名思义是设置发送邮件的时间, 可以选择在什么时间发送。

另一个可选项 Send Emails By是配合Launch Date使用的, Send Emails By代表开始发送时间, Launch Date代表结束发送时间, 所有邮件都会在这个时间段按分钟平均发送。假设这个时间段有10分钟, 那么100封邮件就分成10份, 每一分钟发10份。这样的发件策略可以防止因短时间大量邮件抵达目标邮箱而导致的垃圾邮件检测, 甚至发件邮箱服务器IP被目标邮箱服务器封禁。

New Campaign

Name:

钓鱼邮件测试

Email Template:

钓鱼邮件模板

Landing Page:

钓鱼网页测试

URL: ?

http://117.50.177.71

Launch Date

April 5th 2023, 1:43 pm

Send Emails By (Optional) ?

Sending Profile:

163邮箱

Send Test Email

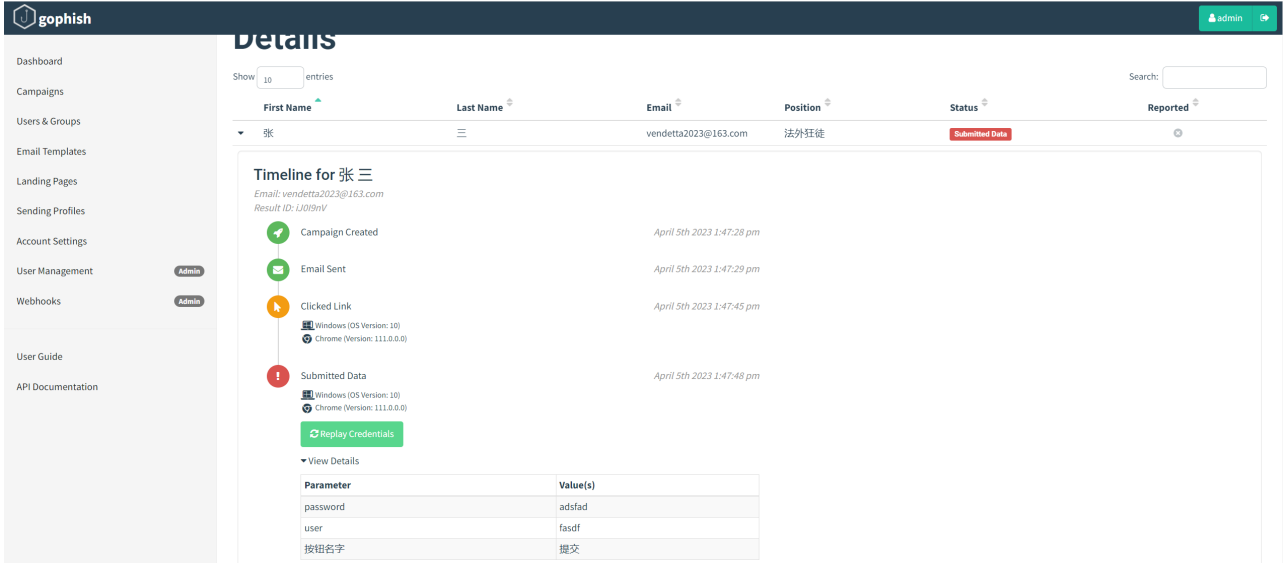
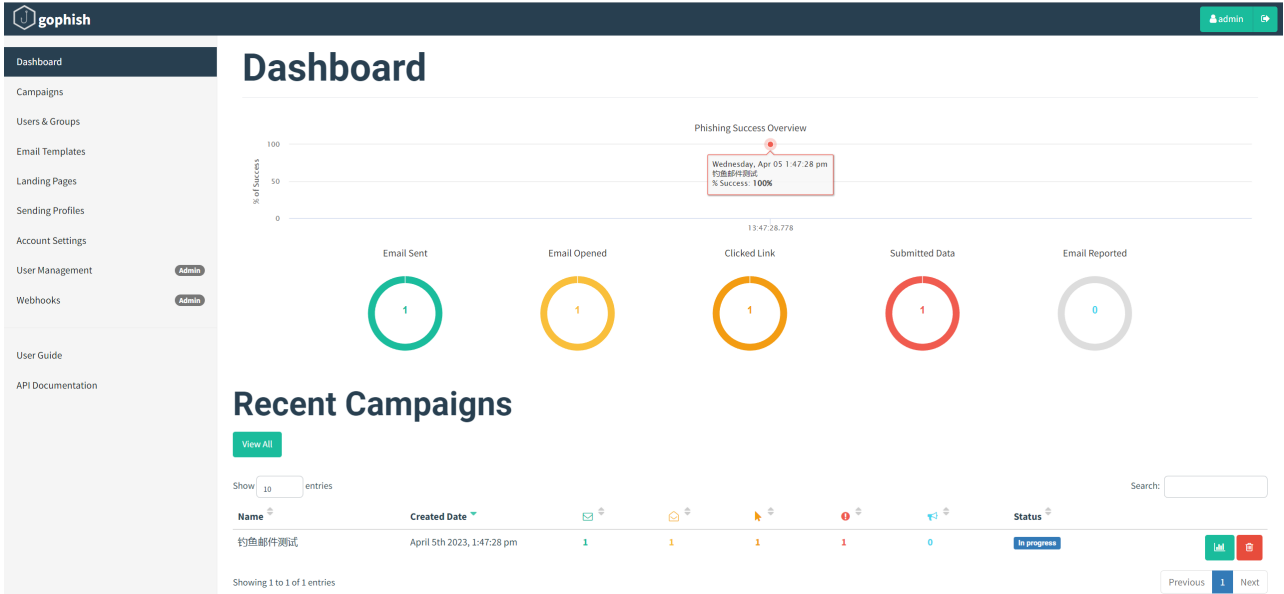
Groups:

× 受害者

Close

Launch Campaign

3.6 攻击结果查看



四、其它参考资料

FREEBUF Jean: <https://www.freebuf.com/articles/network/276463.html>

CSDN 大飞先生: https://blog.csdn.net/m0_63917373/article/details/129931338?csdn_share_tail=%7B%22type%22%3A%22blog%22%2C%22rType%22%3A%22article%22%2C%22rid%22%3A%22129931338%22%2C%22source%22%3A%22m0_63917373%22%7D&fromshare=blogdetail

个人博客 鑫xin哥: <https://www.cnblogs.com/xinssblog/articles/15886097.html>

五、恶意邮件检测

守望者实验室: <https://mailscan.watcherlab.com/search>

六、整站下载工具

小飞兔: <https://www.xftsoft.com/>