

# OneFish使用手册



因为OneFish在快速迭代中，本手册内容有一定的时效性，如果您拿到的是本手册的早期版本，请联系微步的员工获得最新版。

- 本版手册最后更新于2021年4月26日

## 一、蜜罐部署

### Linux环境：

OneFish 使用MySQL数据库，在使用前请确认您已经安装了MySQL，并知道数据库的root密码。

通过下载或挂载磁盘的方式获得onefish管理端安装包，server-linux-amd64.tar.gz

解压缩

```
tar -xzvf server-linux-amd64.tar.gz
```

初始化数据库，OneFish默认db为onefish，相关数据库及建表语句见 db/sql/MySQL.sql 这个文件。

- 在命令行执行下述命令，并输入密码，将db/sql目录下的MySQL.sql添加进数据库。

```
MySQL -u root -p < db/sql/MySQL.sql
```

-- 使用远程连接工具（比如sqlyog等）导入sql脚本的方式也可以。

修改OneFish数据库配置，在config.ini文件中可以进行相关配置。需要将密码OneFish210改为您自己的数据库密码，

默认连接本机127.0.0.1，用户名是root，其他可以自行进行配置。



```
[database]
type = mysql
max_open = 50
max_idle = 50
url = root:OneFish210@tcp(127.0.0.1:3306)/onefish?charset=utf8&parseTime=true&loc=Local
```

做好设置，您可以执行 `./server` 命令运行管理端，当然您也可以使用 `nohup`，让管理端进程后台运行。

```
nohup ./server &
```

补充服务包

管理端自带的Linux-amd64的服务包，如果您有部署其它系统架构节点的需求，请额外下载下面的服务包，并解压到packages目录下。

**#X86架构32位Linux**

<http://hfish.cn-bj.ufileos.com/EP/services-linux-386.tar.gz>

**#ARM架构64位Linux**

<http://hfish.cn-bj.ufileos.com/EP/services-linux-arm64.tar.gz>

**#X86架构32位Windows**

<http://hfish.cn-bj.ufileos.com/EP/services-windows-386.tar.gz>

**#X86架构64位Windows**

<http://hfish.cn-bj.ufileos.com/EP/services-windows-amd64.tar.gz>

**#下载解压示范,请自行替换链接、文件夹路径和包文件名**

```
wget http://hfish.cn-bj.ufileos.com/EP/services-windows-amd64.tar.gz
```

```
cd packages
```

```
tar -xzvf services-windows-amd64.tar.gz
```

新增节点

OneFish想要正常启用，需要依赖节点采集攻击数据。节点端在管理界面即可添加。

详见 [四、节点部署](#)

## Windows环境

OneFish使用了MySQL作为数据库，在运行OneFish前我们需要安装MySQL。

您需要去前往MySQL官网的[下载页面](#)下载MySQL。

### MySQL Product Archives

MySQL Installer (Archived Versions)

**Please note that these are old versions. New releases will have recent bug fixes and features!**  
To download the latest release of MySQL Installer, please visit [MySQL Downloads](#).

Product Version:

Operating System:

<b>Windows (x86, 32-bit), MSI Installer</b> <small>(mysql-installer-web-community-5.7.32.0.msi)</small>	Oct 12, 2020	2.5M	<a href="#">Download</a>
<b>Windows (x86, 32-bit), MSI Installer</b> <small>(mysql-installer-community-5.7.32.0.msi)</small>	Oct 12, 2020	487.5M	<a href="#">Download</a>

We suggest that you use the [MD5 checksums and GnuPG signatures](#) to verify the integrity of the packages you download.

MySQL open source software is provided under the [GPL License](#).

**ORACLE** © 2021, Oracle Corporation and/or its affiliates

[Legal Policies](#) | [Your Privacy Rights](#) | [Terms of Use](#) | [Trademark Policy](#) | [Contributor Agreement](#) | [Cookie 喜好设置](#)

您也可以用下面的链接直接下载我们推荐您推荐的MySQL 5.7版本

```
https://downloads.mysql.com/archives/get/p/25/file/MySQL-installer-community-5.7.32.0.msi
```

### 安装MySQL

安装过程请自行查询，或参考MySQL的官方文档，记住自己的root密码，后面需要用到。

### 下载OneFish

访问我们官网的[下载页面](#)，下载最新版的管理端并解压。

打开cmd，在文件目录运行下面的命令，初始化数据库

```
MySQL -u root -p < db/sql/MySQL.sql
```

给数据库report\_time字段解决权限为空问题

```
sql_mode=strict_trans_tables,no_zero_in_date,error_for_division_by_zero,no_auto_create_user,no_engine_substitution
```

使用远程连接工具（比如sqlyog等）导入sql脚本的方式也可以。

修改文件目录下的config.ini 文件

- 修改123456 为你上面记录的MySQL密码



```
[database]
type = mysql
max_open = 50
max_idle = 50
url = root:0neFish210@tcp(127.0.0.1:3306)/onefish?charset=utf8&parseTime=true&loc=Local
```

运行文件目录下的server.exe

新增节点

OneFish想要正常启用，需要依赖节点采集攻击数据。节点端在管理界面即可添加。

详见 [四、节点部署](#)

## 蜜罐服务说明

目前蜜罐的服务支持6大类，29种不同的标品蜜罐服务，支持vpn溯源蜜饵与真实主机失陷检测。

### 1. 常见的基础服务

包括SSH蜜罐、FTP蜜罐、TFTP蜜罐等六种基础服务蜜罐

### 2. 常见的数据库服务

包括MySQL蜜罐、Redis蜜罐等四种数据库蜜罐

### 3. 常见Web应用仿真

包括常见VPN、企业建站、码云、邮件、OA、HR等10种web蜜罐

天融信防火墙仿真登陆蜜罐、海康摄像头仿真蜜罐、绿盟防火墙仿真登陆蜜罐

#### 4. 常见的网络设备服务

包括常见交换机仿真蜜罐

#### 5. 常见的安全设备服务

包括常见几种防火墙的仿真蜜罐

#### 6. 常见的IOT服务

包括常见摄像机、打印机、主动管理技术仿真蜜罐，其对当前设备界面进行高度还原，诱导攻击者攻击，可收集攻击者邮箱及其远程执行的命令。

#### 7. 自定义服务

CUSTOM蜜罐

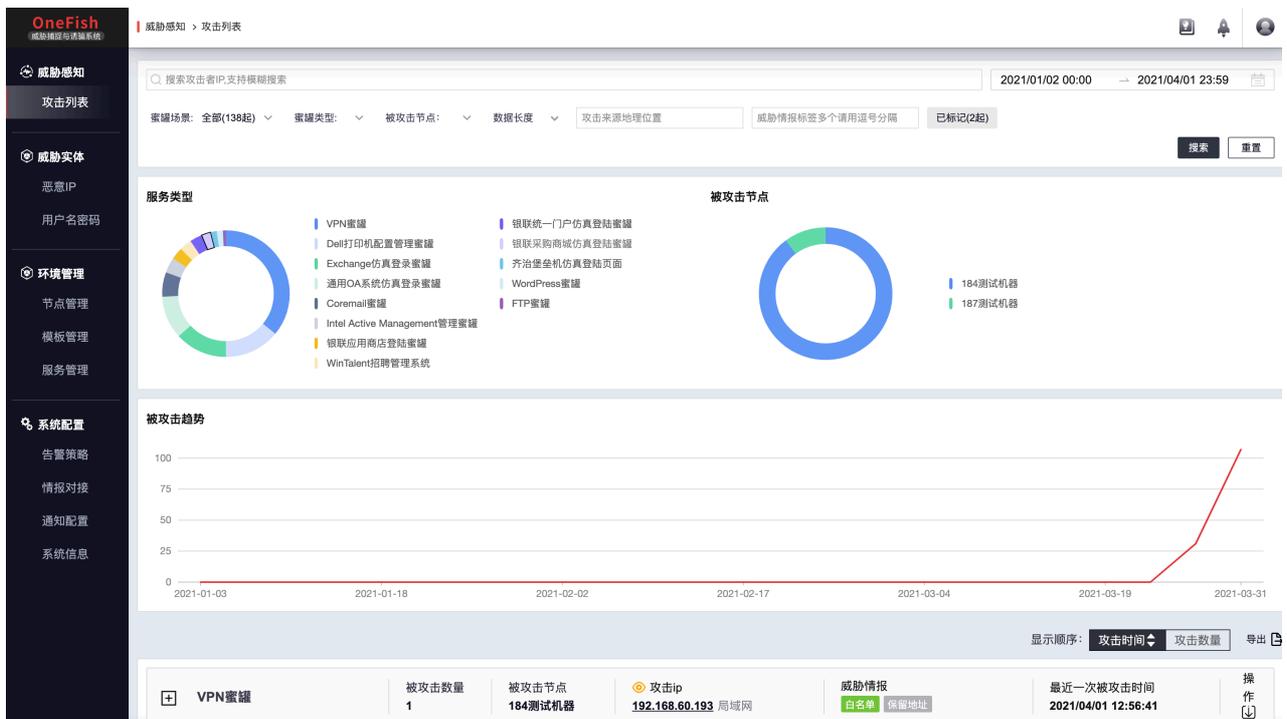
## 二、蜜罐的安全配置

OneFish完整的业务通过管理端和节点共同完成。

管理端是管理所有蜜罐节点的控制台，蜜罐节点会把自己的诱捕、探测到攻击数据回传给管理端。

我们提供了一个web管理页面，大家可以通过这个页面实现对管理端和节点的配置、管理。

在这里能看到所有节点捕获的攻击流量，及微步在线的云端情报能力和数据分析能力，以此辅助用户对攻击者的攻击行为进行研判和溯源。



## OneFish的网络环境

管理端应部署在安全区，只向少部分有网络管理权限和安全分析能力工作的人员和设备开放web和ssh端口

管理端用于配置管理的web页面开启了https，默认访问端口为4433，默认页面在web目录下。（端口和目录，可以在config.ini中自行配置）。

```
# 举例：如果您管理端的ip为192.168.11.11，那么您应该在浏览器中输入如下的URL进行访问。
```

```
https://192.168.11.11:4433/web/
```

此外管理端还会开放默认另外两个端口，节点数据回传端口默认为4434，SSH服务默认访问端口为22。

**4433端口和22端口，“只能”被安全区的管理设备访问。4434端口，“必须能”被蜜罐节点访问。**

OneFish管理端会主动访问如下网络域名

OneFish支持IPv4和IPv6地址环境，可以在完全隔离互联网的内部网络工作，但为了最大限度感知真实威胁和对接云端接口消费威胁情报，以及接受自动化升级服务，微步在线强烈建议客户允许OneFish管理端访问互联网，为兼顾安全性和服务可用性，推荐用户仅允许OneFish管理端主动访问如下网络域名、地址和端口：

目的IP	协议/端口	对应域名	访问目的
103.210.21.74	TCP/443	hfish.io	用于官网升级功能，建议开启。 (如无法开启，可在本地管理端上传升级包进行升级)
106.75.36.224 123.59.72.253 123.59.51.113 106.75.36.226 117.50.17.104	TCP/443	api.threatbook.cn	用于威胁情报查询，如果无需感知威胁情报，则无需开放
该域名使用CDN解析，建议用户在实际网络中解析后开放权限	TCP/443	open.feishu.cn	用于飞书告警功能，如果未使用该功能，无需开放
该域名使用CDN解析，建议用户在实际网络中解析后开放权限	TCP/443	oapi.dingtalk.com	用于钉钉告警功能，如果未使用该功能，无需开放
该域名使用CDN解析，建议用户在实际网络中解析后开放权限	TCP/443	qyapi.weixin.qq.com	用于企业微信告警功能，如果未使用该功能，无需开放

注意：OneFish管理端仅需要通过NAT模式访问互联网，基于安全考虑，微步在线不建议用户将OneFish管理端管理接口暴露在互联网。

1. 如果使用邮件通知，请开启相应邮件服务器的访问权限。
2. 支持 5 路syslog日志的发送，便于您的安全设备联动。请根据自己的情况开放权限。
3. 支持 5 路Webhook的发送，支持对联企业微信、钉钉、飞书，同时兼容自定义url的攻击数据转发。

## 管理端的资源要求

OneFish管理端和客户端支持在复杂环境部署，部署所需硬件环境如下表：

针对我们过往的测试的情况，我们给出两个配置，一个最低配置，一个是我们的推进配置。如果您的蜜罐打算接到公网，并有比较大的攻击流量，请跟进资源占用情况，提升主机的配置。

	OneFish管理端		OneFish节点	
	最低配置	建议配置	最低配置	建议配置
CPU	2核	4核	1核	2核
内存	4G	8G	1G	4G
硬盘	50G	500G	20G	50G

## 管理端的权限审核

对独立中间件和数据库的需求

1. 截止到OneFish2.3.0版，我们不需要独立的中间件。需要MySQL数据库。

对root权限的需求

截止到OneFish2.3.0版，直接部署安装方式管理端的过程中，对于MySQL数据的安装和配置需要root权限。管理端的部署和使用不需要root权限。

## 节点的安全配置

节点因为是直接面对攻击者的，安全配置是节点安全的重要保障

1. 外网节点和内网节点不能共用
2. 如果有节点需要能被外网访问，那么建议把节点和管理端部署在DMZ区。
3. 外网节点除了能访问管理端的4434（默认）端口外，不能有权访问内网中的任何资产。
4. 内网节点除了开放蜜罐服务相应端口外，其它任何端口都不应该在网络中能被用户访问到。考虑安全区设备有维护节点主机的需求，可以向有限的设备开放ssh端口。

## 三、管理端管理

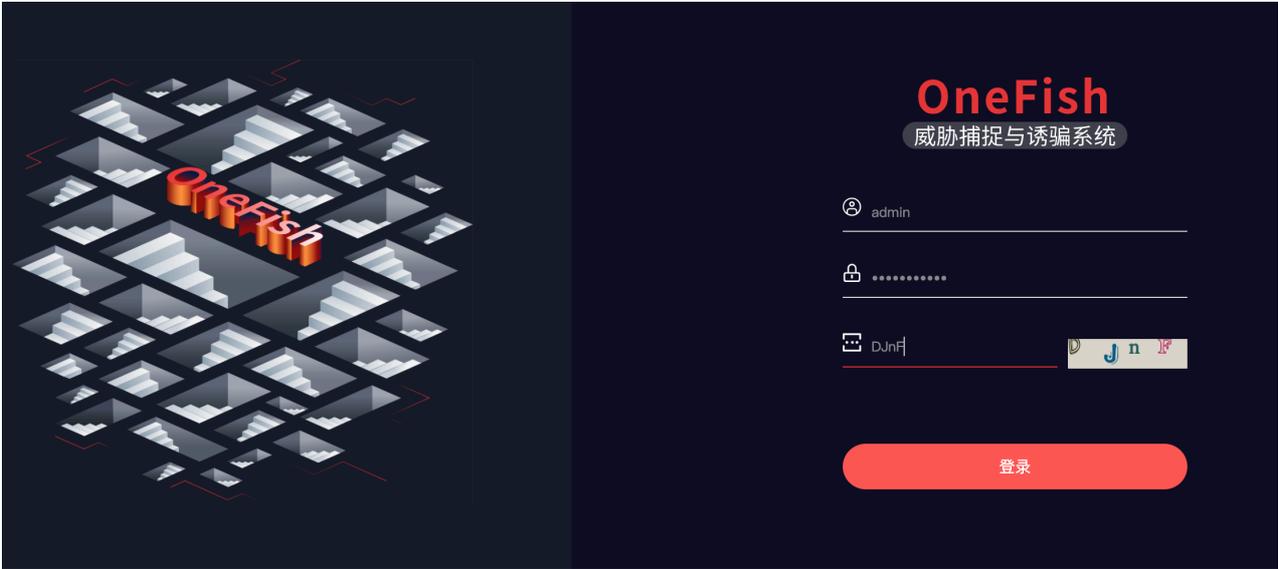
### 默认密码

初次登陆访问

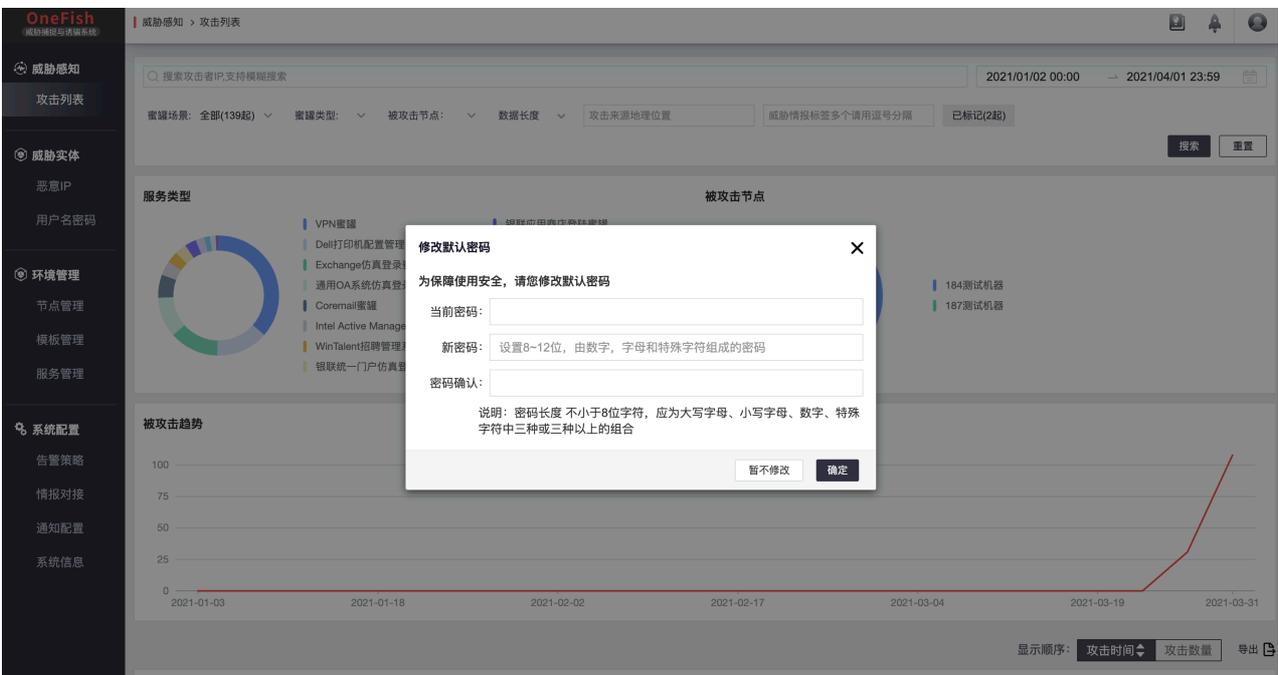
[https://server\\_ip:4433/web/](https://server_ip:4433/web/)

初次登陆账号密码为

admin / OneFish2021



登陆后请及时修改您的密码



# 情报对接

对接精准的云端的威胁情报后，可以对攻击行为进行更准的研判，帮助我们更科学的进行处置。

对接了威胁情报后，当OneFish捕获到了来自外网的攻击行为后，我们可以在攻击列表中了解攻击者的IP情报。OneFish会把您在云端查询到的情报在本地缓存3天，保持您攻击情报时效性的同时，节省您的查询次数。

The screenshot displays the OneFish Threat Intelligence dashboard. The left sidebar contains navigation options: 威胁感知 (Threat Perception), 攻击列表 (Attack List), 威胁实体 (Threat Entities), 环境管理 (Environment Management), and 系统配置 (System Configuration). The main content area shows a list of attacks for 'SSH蜜罐' (SSH Honey Pot). Two entries are visible: one with 49 attacks from IP 143.198.236.231 (USA) and another with 1 attack from IP 62.234.213.198 (China). Below the list is a line chart titled '事件被攻击趋势' (Event Attack Trend) showing a spike in attacks on 2021-03-31. A detailed view of the second attack shows the time 2021/04/01 12:04:49, the IP 62.234.213.198, and the user 'ubuntu6user'.

- 我们支持对接两种来自微步在线的威胁情报

对接微步在线云API (IP信誉接口)

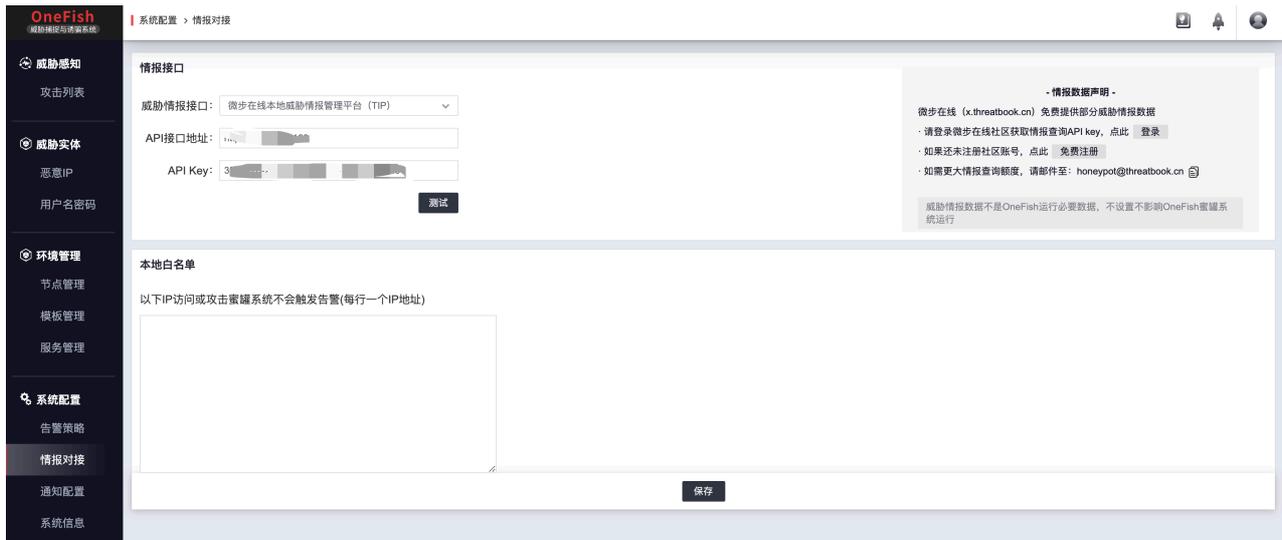
关于该接口完整的说明，可以参考[微步在线云API文档](#)

本接口在注册后可以获得每日50条云端情报的查询额度，给微步发送扩容邮件后，可以提升到每日200条的额度。详情访问[微步在线X社区](#)。

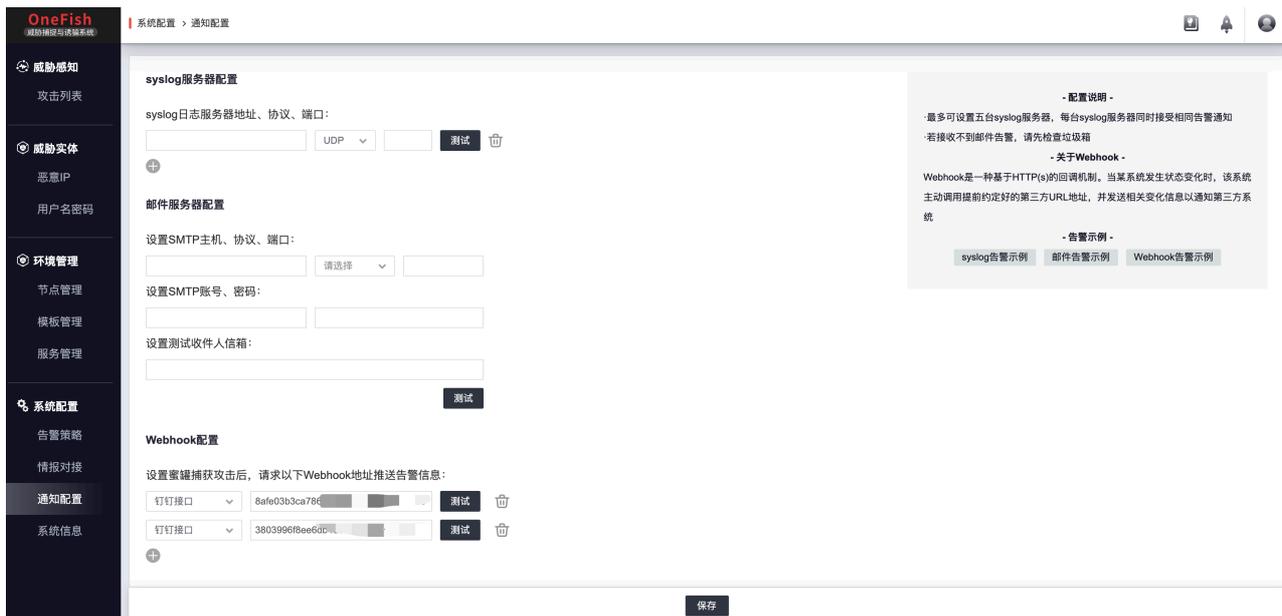
The screenshot shows the '情报对接' (Threat Intelligence) configuration page in OneFish. The '情报接口' (Threat Interface) section is active, showing a dropdown menu set to '微步在线云API (IP信誉接口)'. Below it are input fields for 'API接口地址' (API Interface Address) with the value 'https://api.threatbook.cn' and 'API Key'. A '测试' (Test) button is present. To the right, a '情报数据声明' (Threat Intelligence Data Statement) box contains text about API key requirements and contact information. The '本地白名单' (Local Whitelist) section below has a text area for IP addresses and a '保存' (Save) button.

对接TIP的本地情报，您可以跟据页面的描述进行注册和使用。

使用该接口需要购买微步在线的TIP本地情报系统。



## 通知配置



通知功能是蜜罐的核心功能之一

对于蜜罐捕获到的信息，跟据您不同的安全运营流程，您可能需要把该信息第一时间通知其它的安全设备，也可能需要把该信息通知给相关的安全运营人员。OneFish用三种方式满足您的需求。

- Syslog通知
- 邮件通知
- Webhook通知

## 用 Syslog 联动其它安全设备

您可以自定义接受通知设备的地址、协议和端口，用来接受OneFish捕获的攻击信息和报警。OneFish最多支持5路syslog进行通知。

## 用邮件通知相关安全人员

您可以通过配置相关的邮件服务器信息，来接受OneFish的通知和报警。

## Webhook通知其它设备/人

很多的场景下我们都可以方便的使用webhook联动人或者设备。

- 对于当前企业办公中最为流行的3大即时通讯软件企业微信、钉钉、飞书的机器人，我们也做了适配，您在IM中建立一个机器人，把机器人的token复制到OneFish的webhook配置中，就可以第一时间在IM中获取蜜罐捕获的攻击告警了。
- 三家IM的官方文档如下，您可以对照进行参考

- 企业微信官方文档

[https://work.weixin.qq.com/help?doc\\_id=13376#%E5%A6%82%E4%BD%95%E4%BD%BF%E7%94%A8%E7%BE%A4%E6%9C%BA%E5%99%A8%E4%BA%BA](https://work.weixin.qq.com/help?doc_id=13376#%E5%A6%82%E4%BD%95%E4%BD%BF%E7%94%A8%E7%BE%A4%E6%9C%BA%E5%99%A8%E4%BA%BA)

- 钉钉官方文档

<https://ding-doc.dingtalk.com/doc#/serverapi2/qf2nxq>

- 飞书官方文档

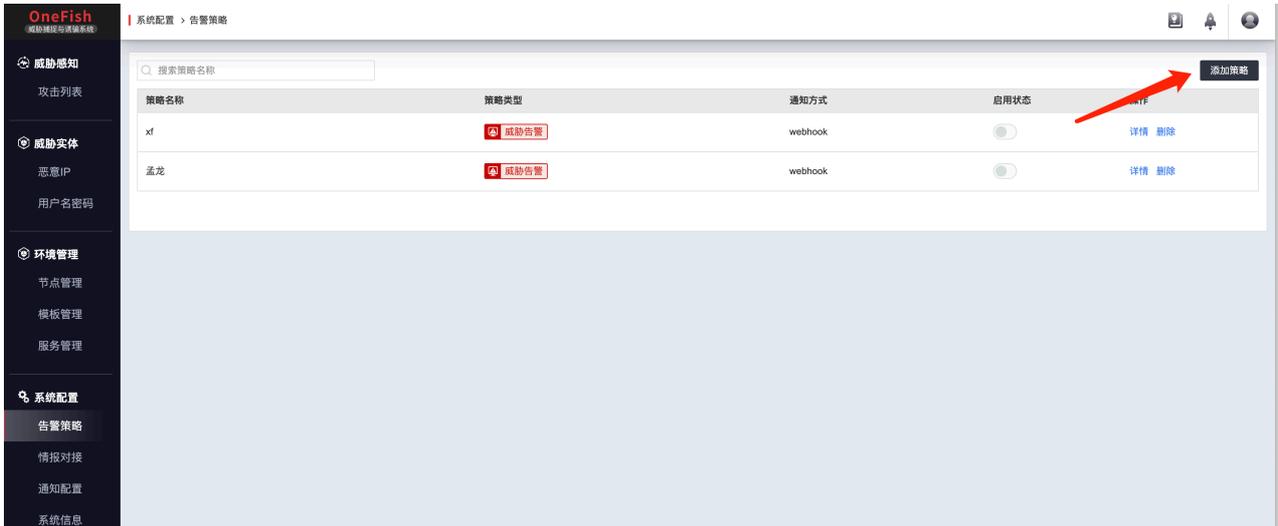
<https://www.feishu.cn/hc/zh-CN/articles/360040553973>

OneFish支持您自定义不同的告警策略。您可以为您不同类型的内容，进行不同方式的通知，以及通知给不同的人。

- 在您配置告警策略之前，您需要先完成上面的【通知配置】

## 告警策略

### 添加一个新的策略



## 对策略进行配置



通知当前分为威胁告警和系统通知两种类型

威胁告警是系统感知攻击时的告警；系统通知是系统自身运行状态的告警。

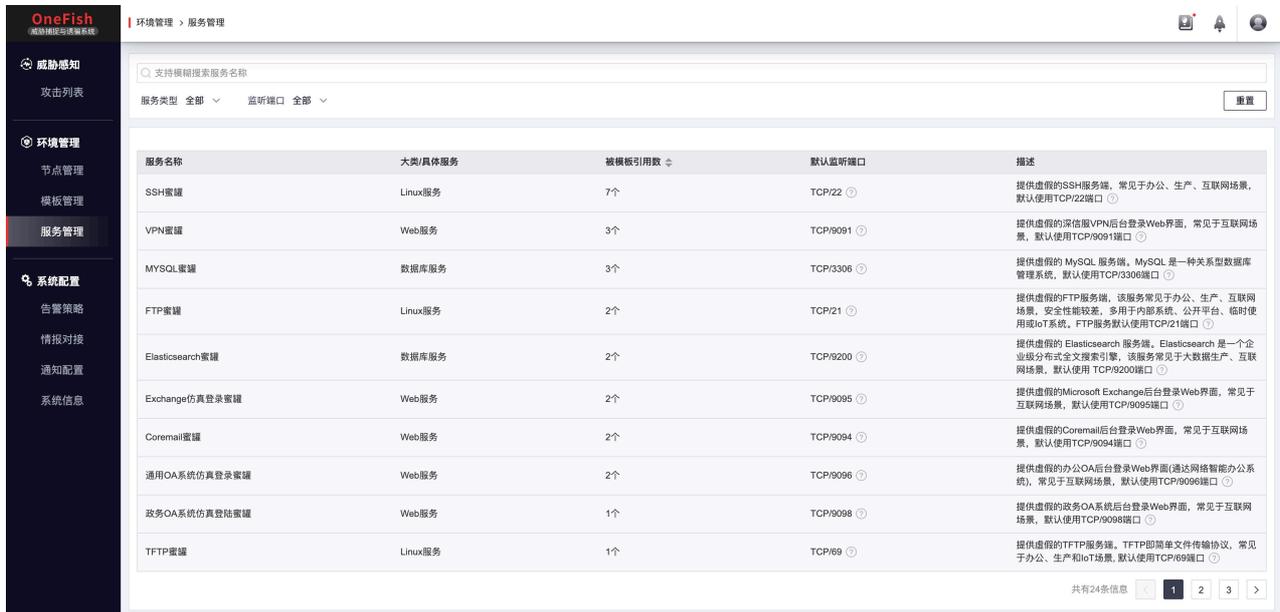
在设置通知方式前，您应该先完成了前边的通知配置

如果您完成了通知配置，那么这里三种不同的通知方式中就会出现您之前的配置，勾选即可。

## 四、节点的部署

### 蜜罐服务

当前OneFish已经支持了26种蜜罐，后续的蜜罐还在不断更新



服务名称	大类/具体服务	被模板引用数	默认监听端口	描述
SSH蜜罐	Linux服务	7个	TCP/22	提供虚假的SSH服务端。常见于办公、生产、互联网场景。默认使用TCP/22端口。
VPN蜜罐	Web服务	3个	TCP/9091	提供虚假的深信服VPN后台登录Web界面。常见于互联网场景。默认使用TCP/9091端口。
MYSQL蜜罐	数据库服务	3个	TCP/3306	提供虚假的MySQL服务端。MySQL是一种关系型数据库管理系统。默认使用TCP/3306端口。
FTP蜜罐	Linux服务	2个	TCP/21	提供虚假的FTP服务端。该服务常见于办公、生产、互联网场景。安全性较差。多用于内部系统、公开平台、临时使用或IoT系统。FTP服务默认使用TCP/21端口。
Elasticsearch蜜罐	数据库服务	2个	TCP/9200	提供虚假的Elasticsearch服务端。Elasticsearch是一个企业级分布式全文搜索引擎。该服务常见于大数据生产、互联网场景。默认使用TCP/9200端口。
Exchange仿真登录蜜罐	Web服务	2个	TCP/9095	提供虚假的Microsoft Exchange后台登录Web界面。常见于互联网场景。默认使用TCP/9095端口。
Coremail蜜罐	Web服务	2个	TCP/9094	提供虚假的Coremail后台登录Web界面。常见于互联网场景。默认使用TCP/9094端口。
通用OA系统的仿真登录蜜罐	Web服务	2个	TCP/9096	提供虚假的办公OA后台登录Web界面(通达网络智能办公系统)。常见于互联网场景。默认使用TCP/9096端口。
政务OA系统的仿真登录蜜罐	Web服务	1个	TCP/9098	提供虚假的政务OA系统后台登录Web界面。常见于互联网场景。默认使用TCP/9098端口。
TFTP蜜罐	Linux服务	1个	TCP/69	提供虚假的TFTP服务端。TFTP即简单文件传输协议。常见于办公、生产和IoT场景。默认使用TCP/69端口。

蜜罐的服务只是魔术师的道具，是否真的能够欺骗到对面的人，使用道具的技巧很重要。

哪些蜜罐服务应该组合在一起？哪些服务应该部署在外网？哪些应该部署在内网？

蜜罐需要跟生产环境完全隔离，还是跟生产环境部署在一台主机上？

反向代理和靶机如何跟蜜罐服务结合，发挥1+1>2的效果？

如何让节点主机在生产网络形成正常的业务数据？如何布撒蜜饵，请攻击者入“罐”.....

如果您需要我们的安全运营针对您的网络为您设计蜜罐方案，请与我们联系。

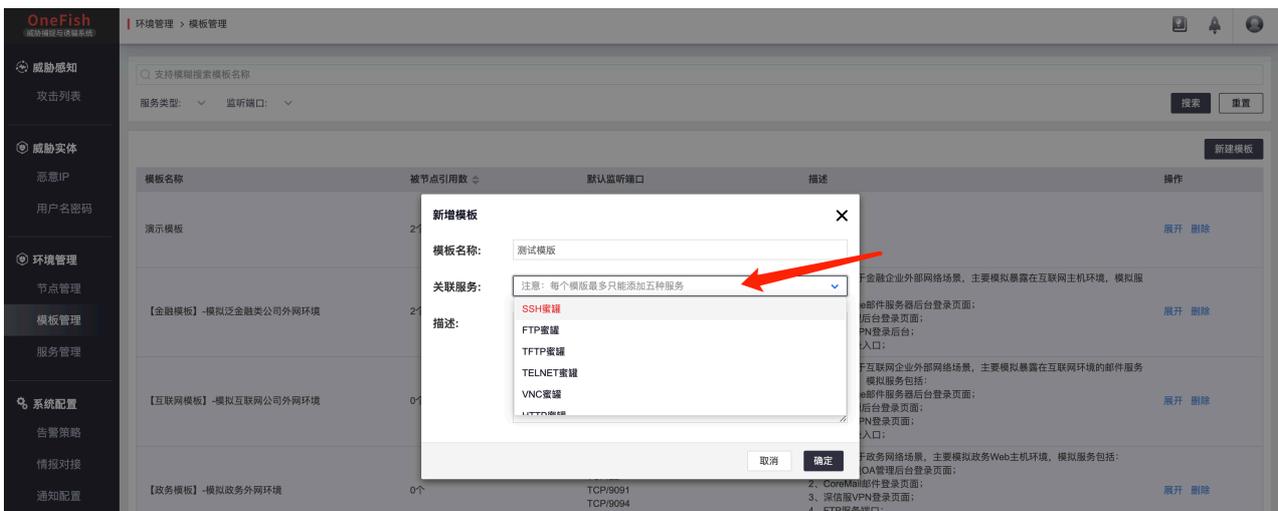
### 新建模板

模板就是几种蜜罐服务的组合，方便您通过给节点部署一个模板，就自动部署上了多种蜜罐

同时多种蜜罐也可以捕获更多的攻击行为。通过组合不同的蜜罐服务，让节点看起来更像是一个真实的业务系统。

这里要一个注意的地方，蜜罐服务并不是部署的越多越好。开放了过多的业务端口，可能会让警惕攻击者觉得可疑。

OneFish自带一些我们推荐的模板，您可以使用。如果您觉得我们的模板不符合您的使用场景，您可以“新建模板”来创建模板。

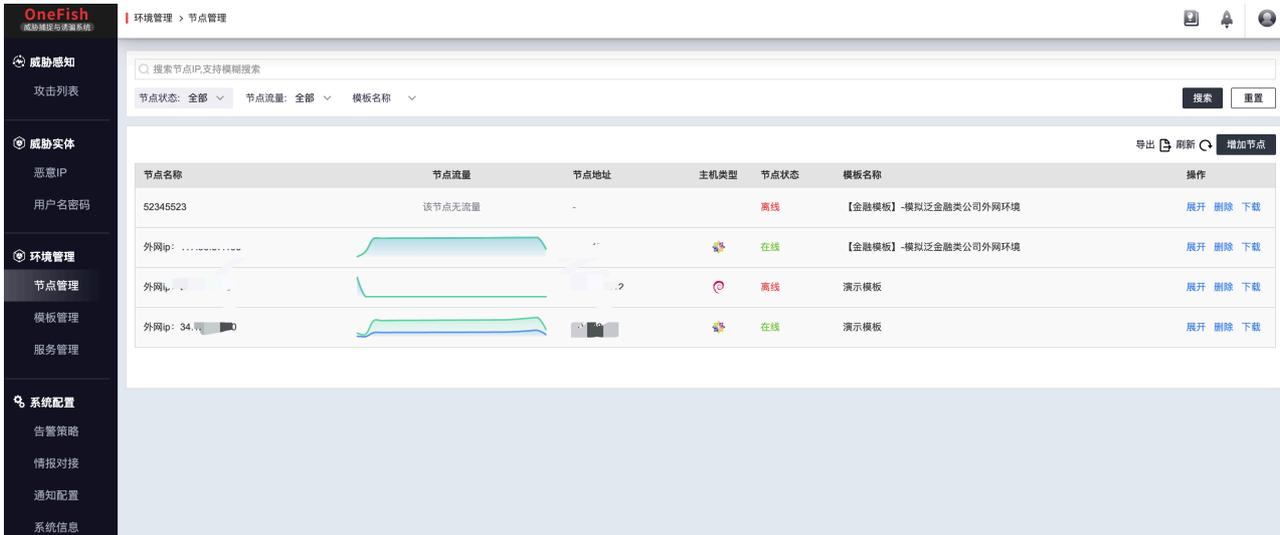


点击新建模板后，选择您想加入模板的服务，每个模板中支持最多添加5个蜜罐服务。

## 新建节点

当您在【模板管理】页面添加完需要的蜜罐模板后，您就可以进行【增加节点】的操作了。

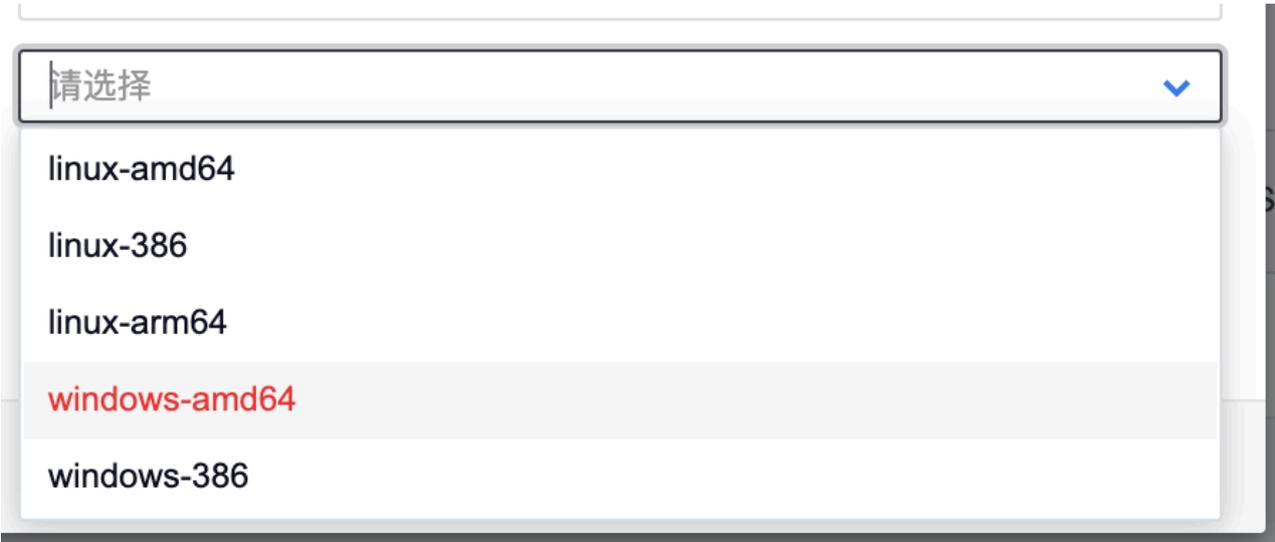
点击增加节点



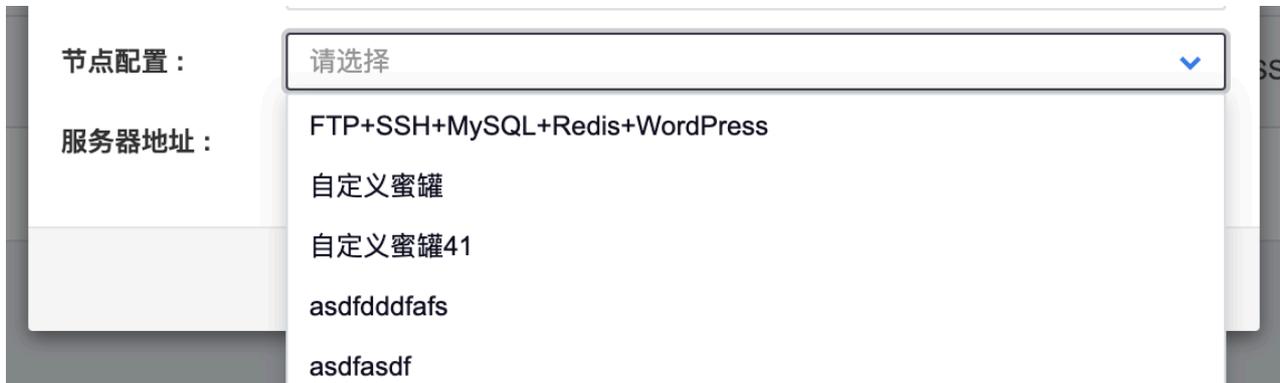
对要增加的节点进行具体的配置



- 节点名称：可以自定义，用于您个人管理中识别设备的名称，长度不低于6个字符
- 部署位置：可以自定义，用于您个人管理中识别设备的位置
- 节点安装包：目前我们支持linux\_x86、linux\_arm、windows，三大平台下的32/64位的设备作为节点，您可以选择相应的版本



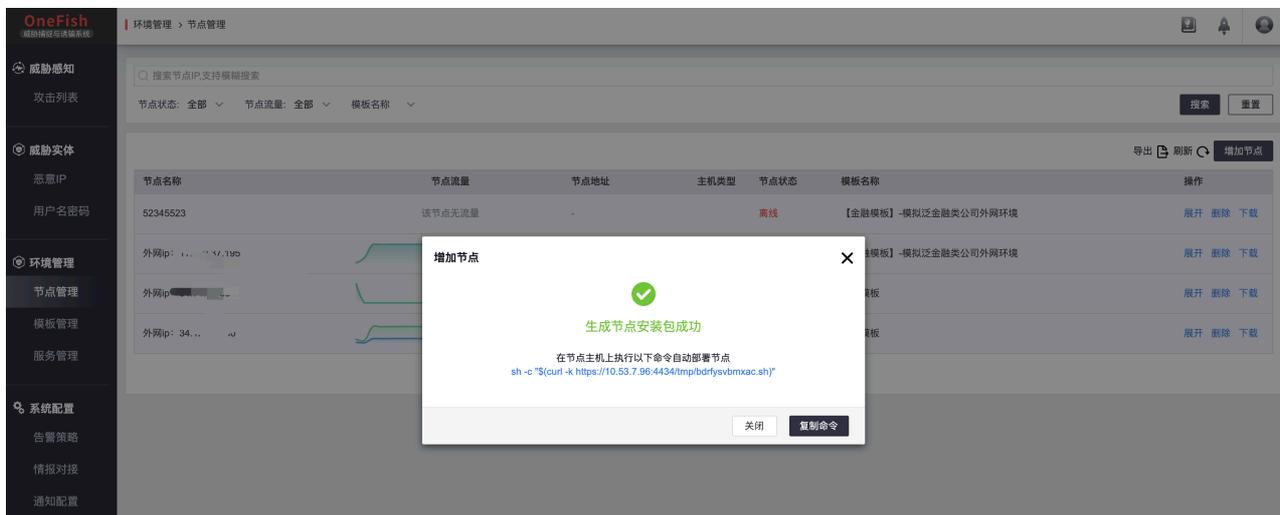
节点配置：节点配置下拉框中，内容就是用户设置的所有模版。此外，节点添加以后仍然可以修改模版。



服务器地址：该服务器地址写您的s端地址，我们支持内网与云主机。请注意一定要注意您的s端地址书写。假设c端添加上长期没有流量，我们建议您查看一下服务器地址是否正确。

## 节点的安装

生成节点成功后，会出现我们的一句话部署命令，点击“复制命令”，并黏贴在节点的命令行下面，节点将自行下载并运行节点的部署脚本。您在管理端上，等待节点上线就可以了。



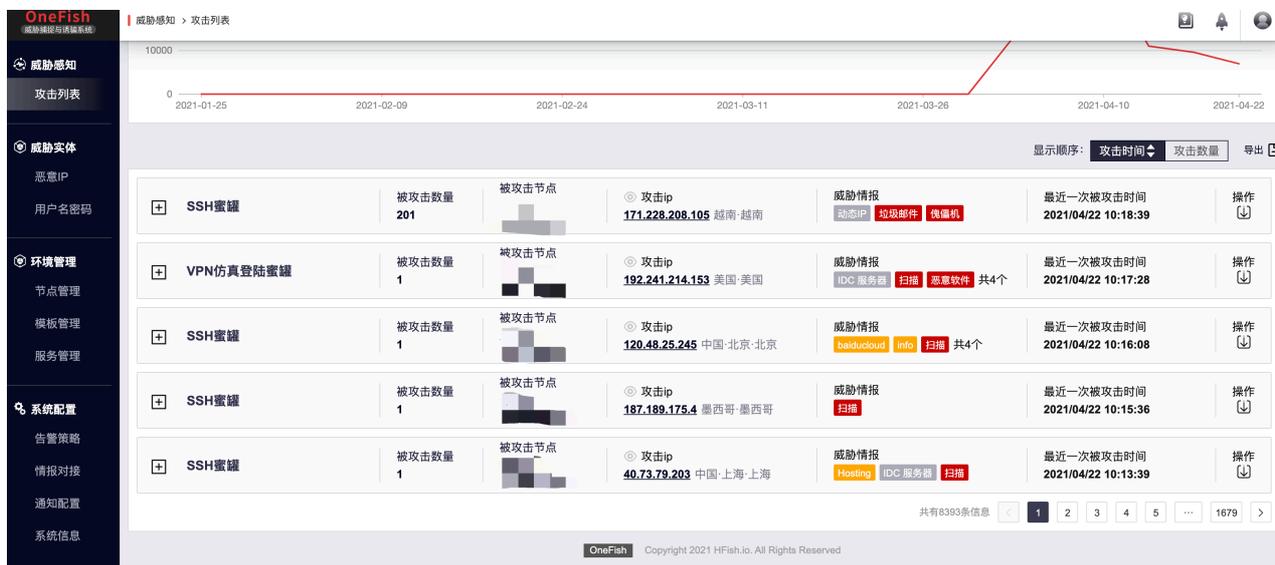
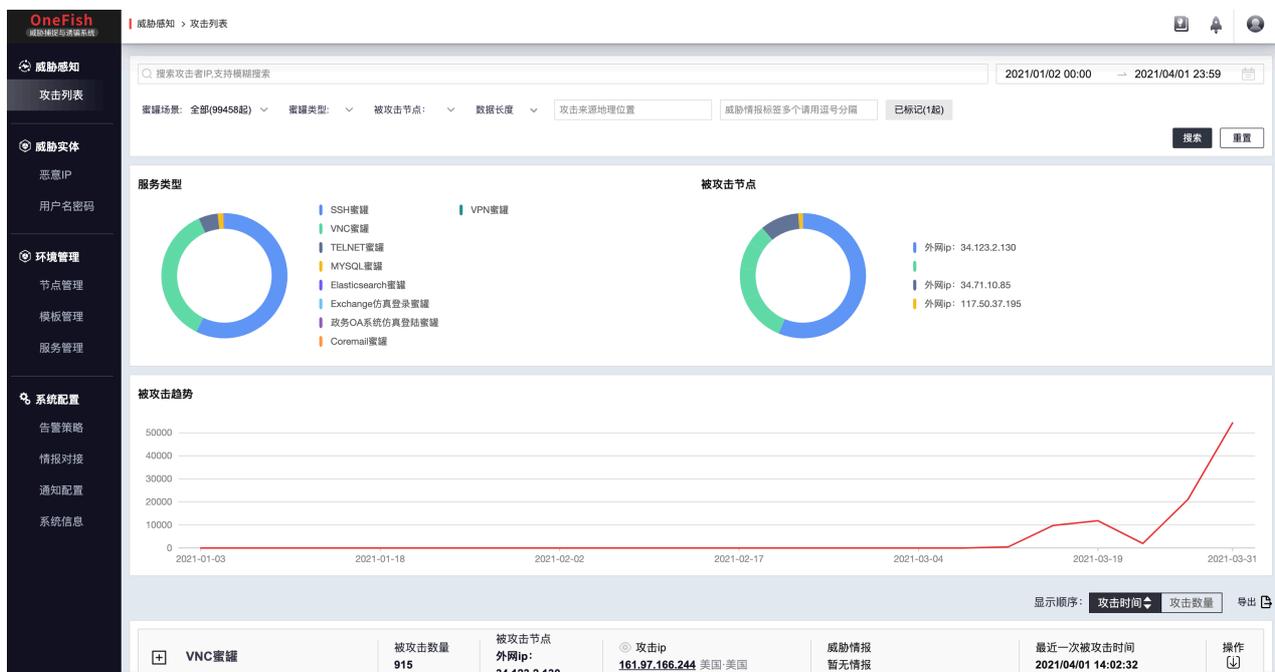
## 注意事项

1. 建议节点是全新的主机环境，除了节点的服务外不要运行其他的任何程序或开放相应的端口。
2. 建议在安装前修改默认的ssh端口，因为ssh蜜罐服务的端口是22，不修改端口的情况下部署ssh蜜罐，会让该蜜罐无法正常启动。
3. 节点的联通性测试结束，正式使用前，记得配置相应的安全策略。SSH 端口，只能被安全区的设备访问。蜜罐管理端口应该对所有网段开放。非蜜罐管理端口应该结束相关进程或调整 iptables&firewalld 规则限制访问。

## 五、界面使用

### 攻击列表

为更好显示数据，攻击列表分为了两个部分。上半轴采用可视化形式，表现出了受攻击情况以及受攻击趋势，下半轴针对攻击日志智能聚合，有效呈现高价值攻击行为及攻击详情。



# 恶意IP

恶意IP页面将监控所有攻击IP的相关信息，包括微步情报及企业自定义情报。

另外，所有的溯源信息，最终都会呈现在恶意IP页面，并成为企业的私有情报库。

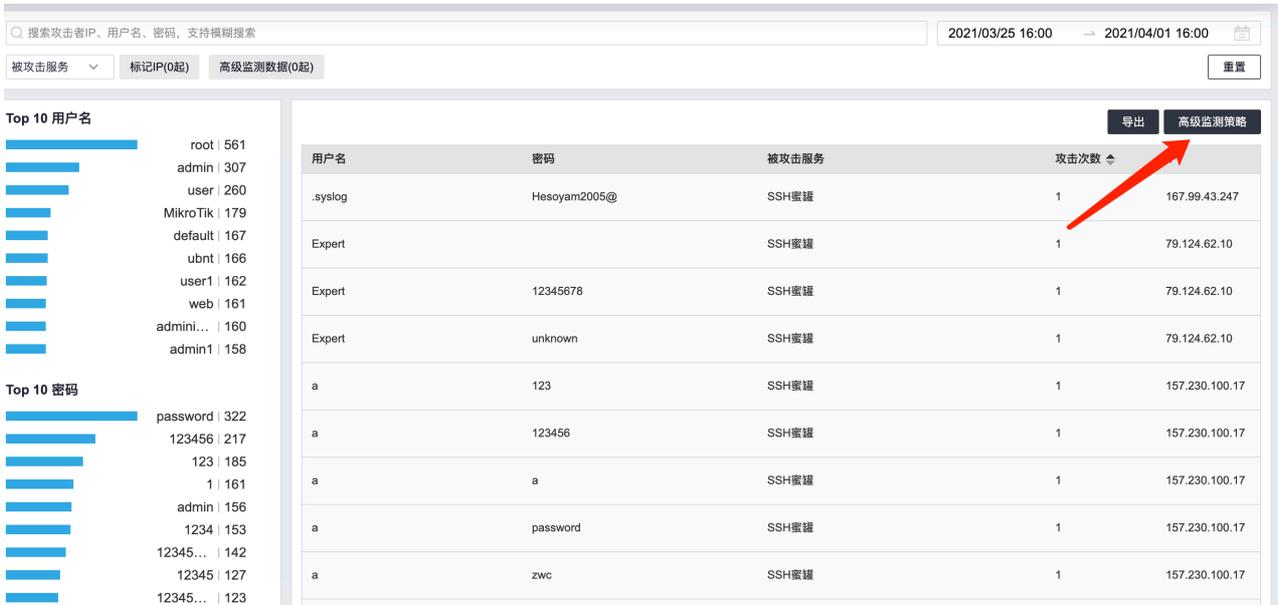
攻击IP	微步情报	自定义情报	攻击服务	攻击节点	溯源信息	操作
39.52.234.116 巴基斯坦 巴基斯坦	动态IP		SSH蜜罐	外网ip: 34.123.2.130	--	📧 👤 🗑️
182.61.133.98 中国 广东 广州	baidcloud Hosting IDC 服务器 共4个		SSH蜜罐	外网ip: 34.123.2.130	姓名: 1. 邮箱: 社交账号: [redacted]	📧 👤 🗑️
61.151.207.141 中国 上海 上海	Hosting 漏洞利用 IDC 服务器 共6个		通用OA系统仿真登录蜜罐	外网ip: 117.50.37.195	--	📧 👤 🗑️
113.160.198.19 越南 越南	暂无情报		SSH蜜罐	外网ip: 34.123.2.130	--	📧 👤 🗑️
39.52.211.219 巴基斯坦 巴基斯坦	动态IP		SSH蜜罐	外网ip: 34.123.2.130	--	📧 👤 🗑️
39.52.192.239 巴基斯坦 巴基斯坦	动态IP		SSH蜜罐	外网ip: 34.123.2.130	--	📧 👤 🗑️
152.136.179.45 中国 北京 北京	Hosting Tencentcloud IDC 服务器 共4个		SSH蜜罐	外网ip: 117.50.37.195	--	📧 👤 🗑️
39.52.195.227 巴基斯坦 巴基斯坦	动态IP		SSH蜜罐	外网ip: 34.123.2.130	--	📧 👤 🗑️
190.85.130.174 哥伦比亚 哥伦比亚	扫描 垃圾邮件		SSH蜜罐	外网ip: 117.50.37.195	--	📧 👤 🗑️
188.166.224.24 新加坡 新加坡	IDC 服务器 扫描 傀儡机		SSH蜜罐	外网ip: 117.50.37.195	--	📧 👤 🗑️

# 账号资产

用户名密码页面收集了所有被用来攻击的账号密码，可以对企业账号资产有效监控

并且，设定高级监测策略，能辅助企业进行内部账号监控，随时监控泄漏情况

用户名	密码	被攻击服务	攻击次数	IP
root	IQ2w3e4r	SSH蜜罐	1	113.219.219.245
root	IQAZ4fv	SSH蜜罐	1	178.128.127.62
root	IQAZ@WSX	SSH蜜罐	1	157.230.100.17
root	IQAZxsw2	SSH蜜罐	1	113.219.219.245
root	IQAZxsw2#EDCvfr4%TGB	SSH蜜罐	1	107.170.134.125
root	I2AQ2wex	SSH蜜罐	1	143.198.236.231
root	!passwd	SSH蜜罐	1	113.219.219.245
root	!qaz@wsx	SSH蜜罐	1	157.230.100.17
root	!root	SSH蜜罐	1	79.124.62.10
root	!(*&*\$#@!	SSH蜜罐	1	143.198.236.231

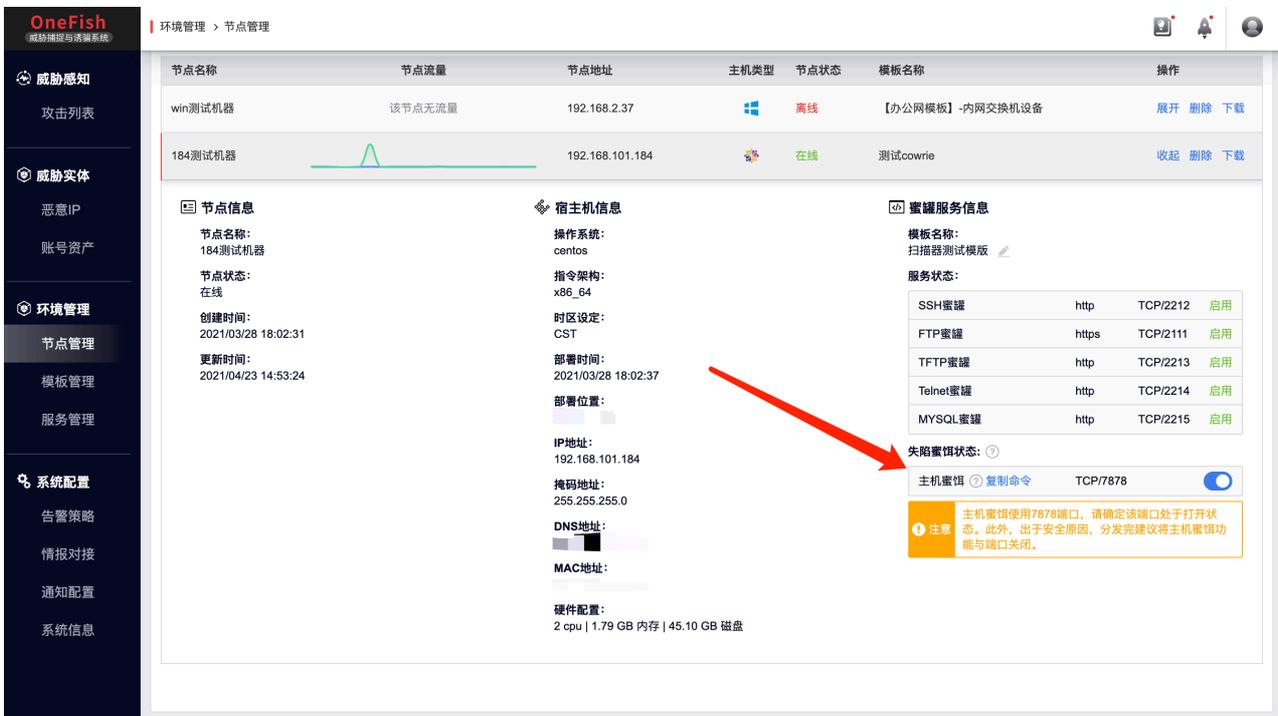


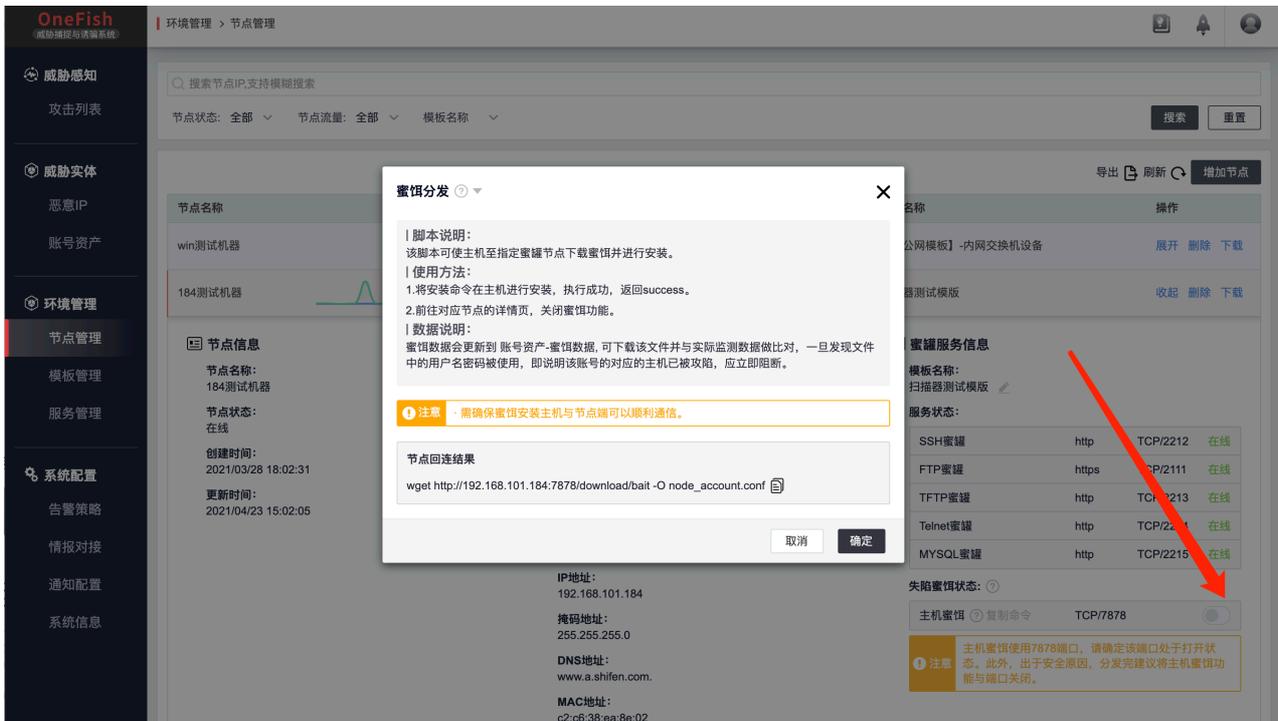
## 主机失陷检测

失陷蜜饵是部署在业务主机上的失陷检测蜜饵。在主机失陷情况下，通过部署虚假的账号、本地证书等失陷蜜饵，诱导攻击者转移攻击目标，并触发失陷告警。

其中，主机蜜饵是一种基于部署虚假的账号密码配置文件，诱导转移攻击者攻击目标的防御手段。

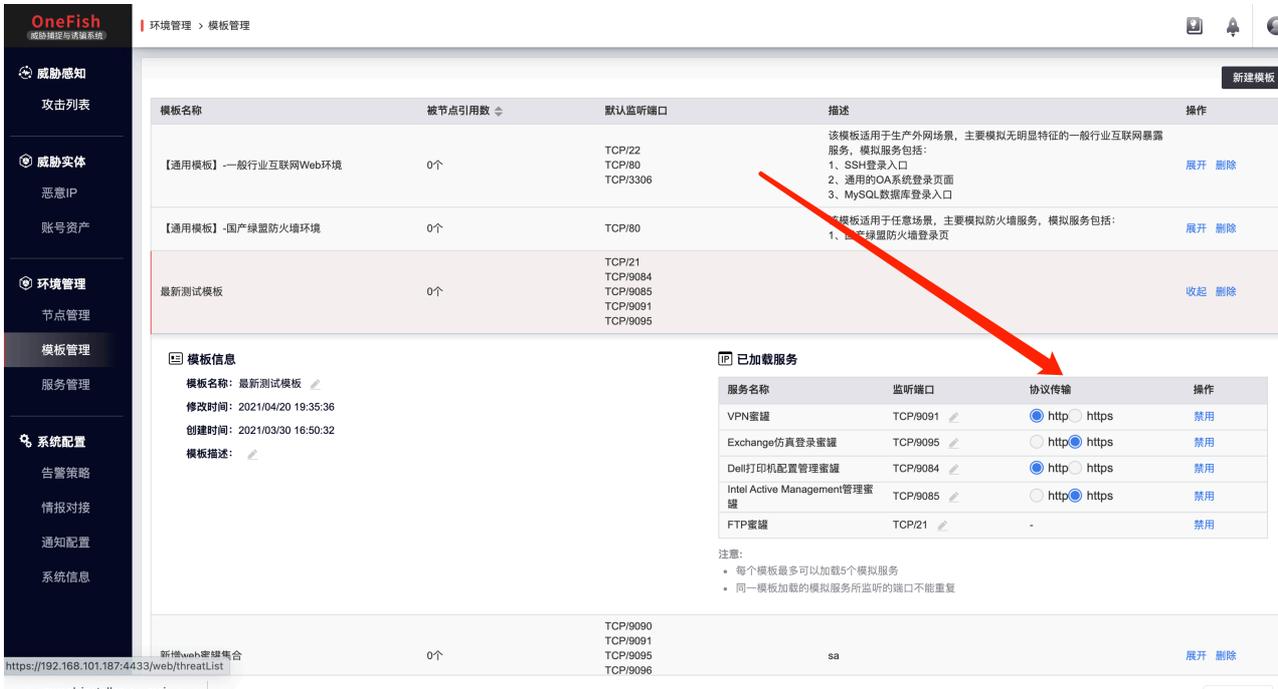
命令在主机运行后，会在本地生成一份虚假的“账号密码备份文件”。当该主机被攻陷时，攻击者将被诱导，使用文件中的账号信息进行登录。借此，安全人员发现主机失陷情况。





## 自定义蜜罐传输协议

针对Web应用仿真、网络设备服务、安全设备服务以及IOT服务, 可以根据自身业务场景和网络情况, 选择其具体的传输协议 (HTTP或者HTTPS), 从而让蜜罐更符合当前网络结构, 更好吸引攻击者视线。



# WEB蜜罐自定义开发

为了方便企业的定制业务，管理段提供了上传自定义web服务的内容，可根据微步在线的开发规范和原则，自己对web界面进行开发，修改，并上传，使其成为真正的蜜罐服务。

如果您希望微步帮助您规范化统一开发，可以与微步在线工作人员进行联系。

The screenshot shows the 'OneFish' interface for 'Service Management'. A table lists various services with columns for name, category, interaction type, template usage, default port, description, and actions. A red arrow points to the '新增服务' button in the top right corner of the table area.

服务名称	大类/具体服务	交互类型	被模板引用数	默认监听端口	描述	操作
SSH蜜罐	基础服务	低交互	15个	TCP/22	提供虚假的SSH服务端，常见于办公、生产、互联网场景，默认使用TCP/22端口	--
FTP蜜罐	基础服务	低交互	8个	TCP/21	提供虚假的FTP服务端，该服务常见于办公、生产、互联网场景，安全性较差，多用于内部系统、公开平台、临时使用或IoT系统。FTP服务默认使用TCP/21端口	--
MySQL蜜罐	数据库服务	低交互	6个	TCP/3306	提供虚假的MySQL服务端。MySQL是一种关系型数据库管理系统，默认使用TCP/3306端口	--
Intel Active Management管理蜜罐	IOT服务	高交互	5个	TCP/9085	提供虚假的Intel Active Management后台管理Web界面，常见于互联网场景，默认使用TCP/9085	预览
HR系统仿真登陆蜜罐	WEB服务	低交互	4个	TCP/9097	提供虚假的HR系统后台登录Web界面，常见于互联网场景，默认使用TCP/9097端口	预览
Exchange仿真登陆蜜罐	WEB服务	低交互	4个	TCP/9095	提供虚假的Microsoft Exchange后台登录Web界面，常见于互联网场景，默认使用TCP/9095端口	预览
WordPress仿真登陆蜜罐	WEB服务	低交互	4个	TCP/9090	提供虚假的WordPress后台登录Web界面，常见于互联网场景，默认使用TCP/9090端口	预览
通用OA系统仿真登陆蜜罐	WEB服务	低交互	3个	TCP/9096	提供虚假的办公OA后台登录Web界面(通达网络智能办公系统)，常见于互联网场景，默认使用TCP/9096端口	预览
Redis蜜罐	数据库服务	低交互	3个	TCP/6379	提供虚假的Redis服务端，常见于生产、互联网场景，默认使用TCP/6379端口	--
VPN仿真登陆蜜罐	WEB服务	低交互 - 蜜饵	2个	TCP/9091	提供虚假的深信服VPN后台登录Web界面，常见于互联网场景，默认使用TCP/9091端口	预览

The screenshot shows the '新增服务' (Add Service) dialog box. It contains the following fields and options:

- Service Name: 请输入不超过32个字符 (支持中英文和数字)
- Service Port: TCP/ 请输入不超过32个字符
- Service Category: 请选择
- Service Description: 请输入不超过500个字符 (0/500)
- Buttons: 上传文件, 取消, 确定

## 六、测试样例

# SSH蜜罐

在终端里，尝试连接蜜罐的ssh端口，会显示“Permission denied, please try again.”

```
water@OneFish ~ % ssh root@192.168.101.184
The authenticity of host '[192.168.101.184] ([192.168.101.184])' can't be established.
RSA key fingerprint is SHA256:A/A19GFe56XEvrorlARWN0ZgXDtYicZ4hcdB7oL66KM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.101.184]' (RSA) to the list of known hosts.
root@192.168.101.184's password:
Permission denied, please try again.
root@192.168.101.184's password:
Permission denied, please try again.
root@192.168.101.184's password:
root@192.168.101.184: Permission denied (password).
```

这时攻击列表会记录下所有测试过的用户名和密码

The screenshot shows the OneFish dashboard interface. On the left is a navigation sidebar with categories like '威胁感知' (Threat Perception), '环境管理' (Environment Management), and '系统配置' (System Configuration). The main area displays '攻击列表' (Attack List) for 'SSH蜜罐'. It includes a line chart for attack trends, a summary table, and a detailed log table. A '详情' (Details) panel is open for the most recent attack, showing the credentials 'root&&admin'.

攻击时间	攻击节点	攻击IP	数据长度	操作
2021/03/11 15:45:26	184测试机器	192.168.61.35 局域网	11字节	☆ 🗑️
2021/03/11 15:45:23	184测试机器	192.168.61.35 局域网	12字节	☆ 🗑️
2021/03/11 15:45:15	184测试机器	192.168.61.35 局域网	10字节	☆ 🗑️
2021/03/11 15:44:09	184测试机器	192.168.61.35 局域网	48字节	☆ 🗑️

# FTP蜜罐

用FTP终端尝试连接FTP蜜罐端口，会在攻击列表中出现FTP蜜罐报警

OneFish 威胁感知 > 攻击列表

显示顺序: 攻击数量 攻击时间 导出

FTP蜜罐 被攻击数量: 2 被攻击节点: 184测试机器 攻击ip: 192.168.61.35 局域网 威胁情报: ERR\_RESP 最近一次被攻击时间: 2021/03/11 16:26:41

事件被攻击趋势

攻击时间	攻击节点
2021/03/11 16:26:41	184测试机器
2021/03/11 16:26:41	184测试机器

已选中0条

## HTTP蜜罐

HTTP蜜罐为http代理蜜罐，利用http代理工具连接蜜罐端口

```
water@OneFish ~ % http_proxy=http://192.168.101.184:80 curl http://hfish.io
```

```
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.16.1</center>
</body>
</html>
```

攻击列表中的显示信息如下

OneFish 威胁感知 > 攻击列表

显示顺序: 攻击时间 攻击数量 导出

HTTP蜜罐 被攻击数量: 1 被攻击节点: 184测试机器 攻击ip: 192.168.61.35 局域网 威胁情报: ERR\_RESP 最近一次被攻击时间: 2021/03/11 16:44:52

事件被攻击趋势

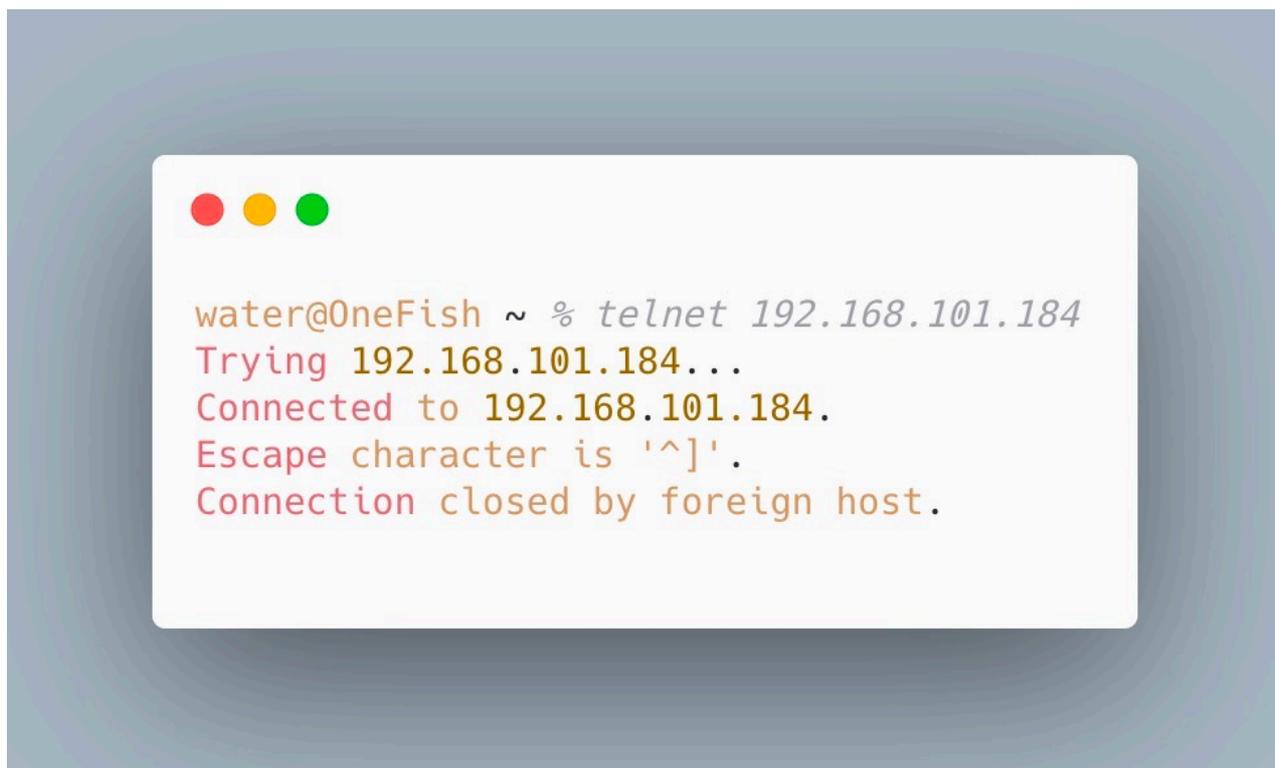
攻击时间	攻击节点	攻击IP	数据长度	操作
2021/03/11 16:44:52	184测试机器	192.168.61.35 局域网	161字节	☆ 导出

详情

URL:http://hfish.io/&&Method:GET&&RemoteAddr:192.168.61.35  
{"Accept":["/\*/\*"],"Proxy-Connection":["Keep-Alive"],"User-Agent":["curl/7.64.1"]}&&Body:

# TELNET蜜罐

利用TELNET应用连接蜜罐端口



攻击列表中显示信息如下

攻击时间	攻击节点	攻击IP	数据长度	操作
2021/03/11 16:52:25	184测试机器	192.168.61.35 局域网	38字节	☆ 消息

192.168.61.35:63841 already connected.

# MySQL蜜罐

用MySQL工具连接蜜罐对应端口

```
water@OneFish ~ % mysql -h192.168.101.184 -uroot -p
Enter password:
ERROR 1130 (HY000): Host '192.168.80.180' is not allowed to connect to this MySQL server
# mysql -h192.168.101.184 -P33306 -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.5.53

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

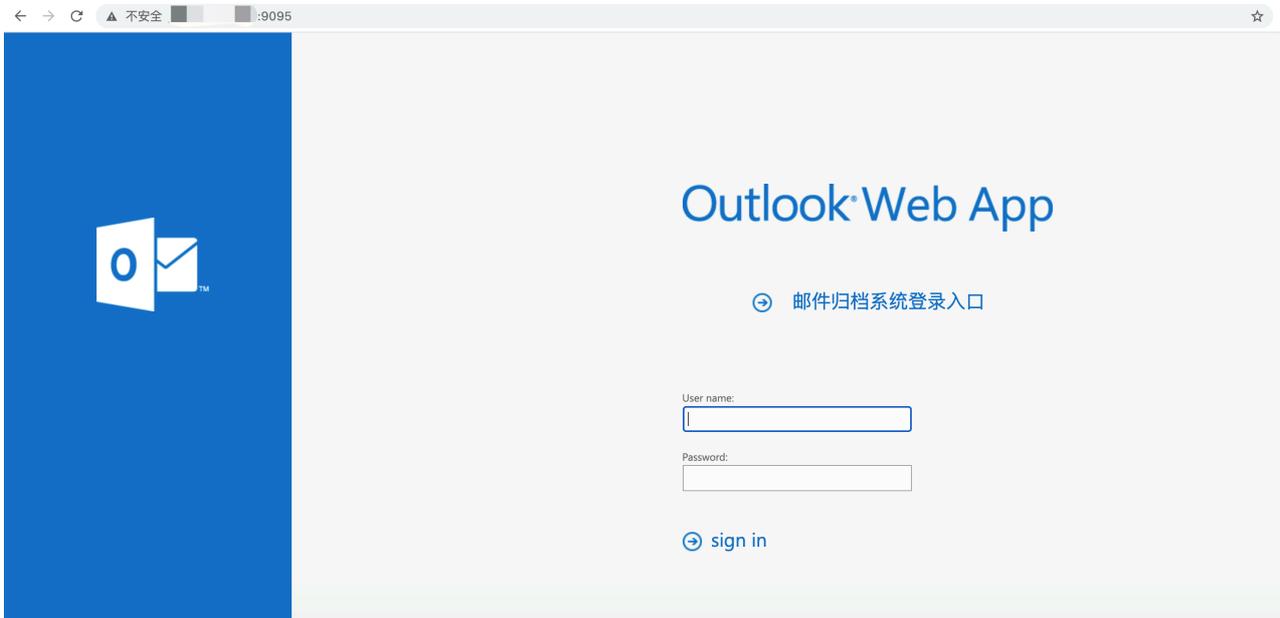
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

## WEB蜜罐

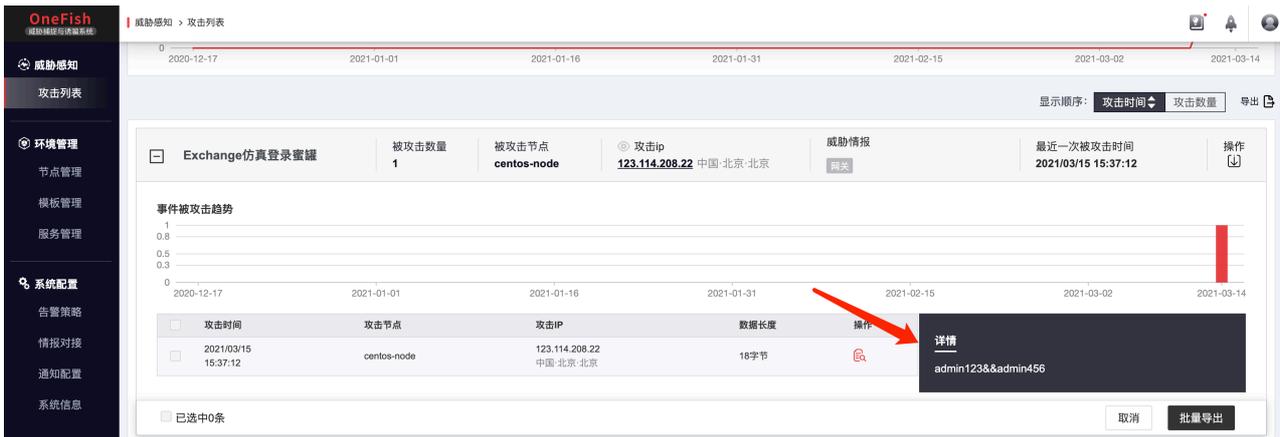
用浏览器访问相应的端口，并尝试输入user name和密码后



会提示用户名和密码错误



管理端后台会获取攻击者用于尝试的用户名和密码



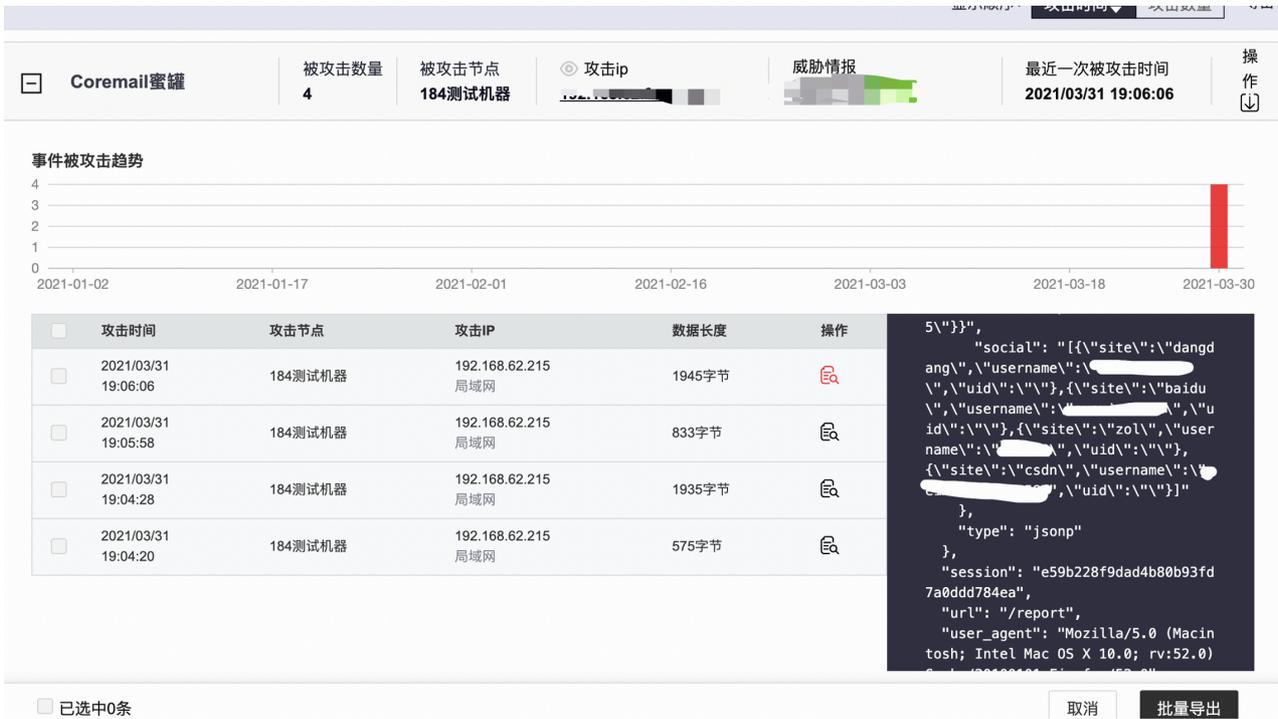
## VPN蜜饵

VPN下载链接会挂在web页面，吸引攻击者下载并使用，并拉取回传攻击者微信账号信息，进行精准溯源。

The screenshot shows a '溯源信息' (Source Information) form. The form contains the following fields: 姓名: 10., 电话: [edit icon], 邮箱: [edit icon], 微信: [edit icon], 社交账号: 3 [edit icon] 4 [edit icon]. Below the form, there is a file link: 文件: [ba02fa996d1d41ccb760da9ed1599bde.zip](#). A red arrow points from the '社交账号' field to the file link. The form also includes a '备注' (Remarks) field with an edit icon.

## 社交信息反查

可在攻击者访问时，反查溯源拿到对方的社交账号（包括百度、亚马逊、csdn...）。



## 七、自定义web蜜罐页面

### web蜜罐文件所在目录

- index.html

在节点client安装目录./services/service\_id/root 下面

- 其它格式的文件

在节点client安装目录./services/service\_id/root下的所有目录都可以自行定义、上传文件，用户可以在不同目录下面上传自己的样式文件和图片。

### 修改页面元素

根据index.html文件中的信息，替换和修改相关的文件。

### 制作全新的登陆页面

我们可以自己制作一个全新的登陆页面，通过替换表单元素实现“定制开发”

- 删除client安装目录./services/service\_id/root下所有文件后，自行上传编辑完成的html页面和相关文件
- 修改主页文件名为index.html
- 按照下面图片的要求，修改表单元素。

密码登录 | 手机登录

用户名或密码不正确

admin

密码

登录

Network: /login x Headers Preview Response Initiator Timing Cookies

Form Data

loginMethod: 0

rememberMe: false

username: admin

password: Db/BJxLxjRS269f94aH8tg==

form 表单形式提交，参数要有username和password,需要小写

## 八、常见问题排查

节点红色离线而蜜罐服务却是绿色的启用?

OneFish 威胁捕捉与诱捕系统

环境管理 > 节点管理

节点状态: 全部 | 节点流量: 全部 | 模板名称: 全部

节点名称: 34.123.2.131 | 节点流量: 该节点无流量 | 节点地址: - | 主机类型: - | 节点状态: 离线 | 模板名称: 【金融模板】-模拟泛金融类公司外网环境 | 操作: 收起 删除 下载

节点信息

节点名称: 34.123.2.131

节点状态: 离线

创建时间: 2021/03/26 11:39:35

更新时间: 2021/03/26 11:39:35

宿主机信息

操作系统:

指令架构:

时区设定:

部署时间: -

部署位置: 外网

IP地址:

掩码地址:

DNS地址:

MAC地址:

硬件配置: 0 cpu | 0 内存 | 0 磁盘

蜜罐服务信息

模板名称: 【金融模板】-模拟泛金融类公司外网环境

服务状态:

SSH蜜罐	TCP/22	启用
VPN蜜罐	TCP/9091	启用
Exchange仿真登录蜜罐	TCP/9095	启用
通用OA系统仿真登录蜜罐	TCP/9096	启用

解决办法：

1. 检查节点到管理端的网络连通情况，并等待.....

```
节点每90秒连接server的4433端口一次，180秒内连接不上，即显示离线。  
在刚刚完成部署，或网络不稳定的时候会出现这种情况。  
这种时候等2~3分钟，如果节点恢复绿色在线，那通常过一会儿，蜜罐服务也会从绿色的启用，变成绿色的在线。
```

2. 检查管理端防火墙以及ACL策略是否放行了节点对server 4434端口访问的权限

```
#可以用wget进行测试  
wget 127.0.0.1:4433
```

3. 如果确认网络访问正常，节点在server那里始终离线，需要检查节点上的进程运行情况。如果进程运行异常，需要杀死全部关联进程后，重启进程，并记录错误日志。

```
#检查./client的进程是否运行正常  
ps aux | grep client  
  
#检查./service的进程是否运行正常  
ps aux | grep service
```

server部署完成后，web页面始终无法打开

解决办法：

1. 确认server进程的运行情况和4433端口开放情况，如果不正常需要重启server进程，并记录错误日志

```
#检查./server的进程是否运行正常  
ps aux | grep server  
  
#检查端口是否正常开放  
ss -ntpl  
  
#节点端日志在安装目录下client/logs文件夹内，文件名称为  
client.log  
  
#蜜罐服务的日志在节点端安装目录下client/service/蜜罐id 文件夹，文件名称为  
蜜罐id.log
```

2. 检查堡垒机是否开放了对server4433端口的访问

节点在线，部分蜜罐服务在线，部分蜜罐服务离线

解决办法：

## 1. 确认蜜罐服务进程是否还在运行?

#检查./service的进程是否运行正常

```
ps aux | grep service
```

#如果进程确实挂了，查看服务的日志

## 2. 确认是否端口冲突?

这个问题常见默认22端口的ssh服务，刚启动client的时候，服务在线，过了一会儿后服务离线。

用`ss -ntpl`检查该蜜罐服务的端口是否被占用?

如果被占用，建议修改该业务的默认端口。

如果在部署节点前，先安装部署流程运行了`node.sh`脚本的话，那么原则上22端口应该不会冲突。但是之前在hbyc的客户现场发现，客户系统中默认的ssh端口不是由`sshd.service`监听的，而是`ssh.socket`提供的。我的脚本就无效了。

### 变更服务模板后，蜜罐新服务访问不到

在OneFish当前的产品结构中，管理端永远不会主动连接节点进行节点配置的变更。

而是在管理端上，生成一个配置，等待节点来拉取。

节点每90秒尝试连接管理端一次，获取到变更数据后，还需要从管理端上拉取新的服务，解压服务包并运行。

运行服务的结果，会在下一个90秒回连时，上报到管理端。

这个流程最慢的话，可能会有一个3分钟左右延时。

所以刚刚变更蜜罐服务后，请大家稍微等等。