ThreatBook
微步在线

威胁诱捕与诱骗系统（HFish）
推荐处置手册

微步在线科技有限公司
LEADER IN THREAT DETECTION AND RESPONSE

目录

一、 产品介绍

HFish 是一款蜜罐工具，侧重企业安全场景，从内网失陷检测、外网威胁感知、威胁情报生产三个场景出发，为用户提供可独立操作且实用的功能，通过安全、敏捷、可靠的中低交互蜜罐增加用户在失陷感知和威胁情报领域的能力。

HFish 具有超过 40 种蜜罐环境、提供云蜜网、可高度自定义的蜜饵能力、一键部署、跨平台多架构、国产操作系统和 CPU 支持、极低的性能要求、邮件/syslog/webhook/企业微信/钉钉/飞书告警等多项特性，帮助用户降低运维成本，提升运营效率。

二、安全检测配置项

2.1 内网推荐配置

以下介绍内网部署时候的推荐部署项

2.1.1告警通知

HFish 支持 Syslog 服务器，邮件与 Webhook 告警配置。

其中 Syslog 服务器与 Webhook 告警配置服务器为实时发送。邮件告警每 10 分钟发放一次。在内网环境中，

Syslog 可以与

- 微步产品 TDP 对接，使其感知内网告警
- 与 SOC、SIEM、Soar 等设备对接，增加精准告警数据源，编排等
- 自定义与内网防火墙对接，自动封禁

Webhook 默认内置对钉钉、飞书、企业微信的支持。

详细配置方式可查看：

https://hfish.net/#/6-2-1dingtalk

https://hfish.net/#/6-2-2wechat

https://hfish.net/#/6-2-3lark

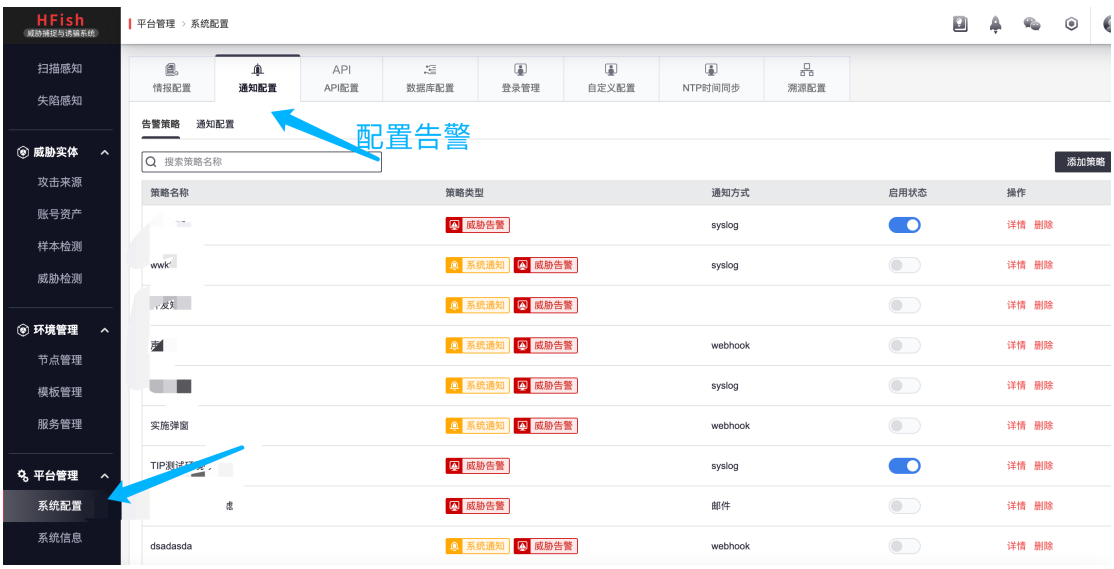

图 告警策略界面示意

其中，基于内网情况，我们建议在选择告警配置的时候，将所有等级的攻击都选择发送。

图 内网策略添加

2.1.2 定期刷新

基于内网监控需求，HFish 提供自动刷新配置，可以自动刷新告警页面的告警数据，方便实时监控。

图 自动刷新功能介绍

2.1.3 白名单配置

2.2 外网推荐配置

以下介绍外网部署时候的推荐部署项。

在外网受攻击情况可显著看出，在识别攻击行为以及预测攻击行为上，HFish 可以有效的吸引恶意攻击，并且提前为企业做出预警。我们建议，企业内可赋予子域名或者更多不同网段的外网 IP 提供给 HFish，构建完整的攻击感知链条与自动化动态封禁防护。

2.2.1告警通知

HFish 支持 Syslog 服务器，邮件与 Webhook 告警配置。

其中 Syslog 服务器与 Webhook 告警配置服务器为实时发送。邮件告警每 10 分钟发放一次。在外网环境中，

Syslog 可以与

- 微步产品 TIP 产品对接，生成私有情报
- 与 SOC、SIEM、Soar 等设备对接，增加精准告警数据源，编排等
- 自定义与内网防火墙对接，自动封禁

外网环境告警过多，建议不要直接配置 Webhook 通知，建议选择邮件告警，发送有一定威胁级别的告警。

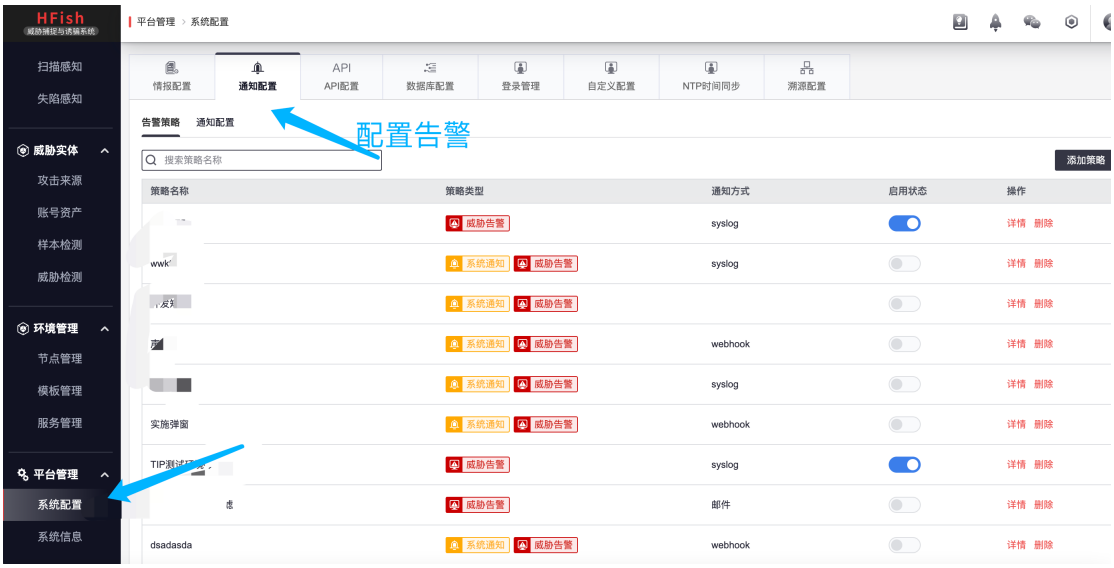

图 告警策略界面示意

其中，基于外网情况，我们建议在选择告警配置的时候，选择有危险等级的告警。

图 外网策略添加

2.2.2 定期刷新

基于外网监控需求，HFish 提供自动刷新配置，可以自动刷新告警页面的告警数据，方便实时监控。

2.2.3 情报对接

基于外网对情报的需求，hfish 提供与微步在线本地威胁情报平台（TIP）产品与 X 情报社区进行情报对接

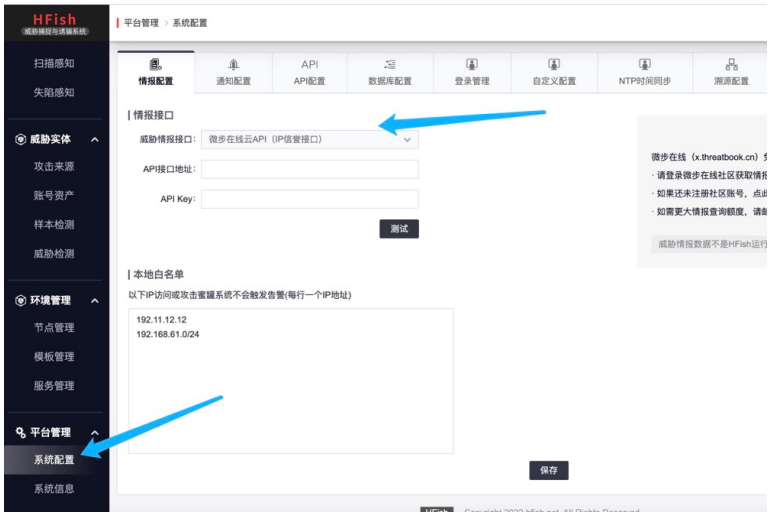

图 HFish 配置情报对接

所有用户在 X 社区，每天有 50 次免费 IP 信誉查询额度可使用，详情可查看：https://x.threatbook.cn/v5/apiDocs

三、重点攻击情况发现

3.1 攻击列表

HFish 在攻击列表中，基于攻击 IP、被攻击节点、被攻击蜜罐三者做了聚合。将聚合后的被攻击次数显示出来。攻击次数在外网可以用来做攻击强度封禁规则。

每一条数据点击可以查看详细攻击数据。

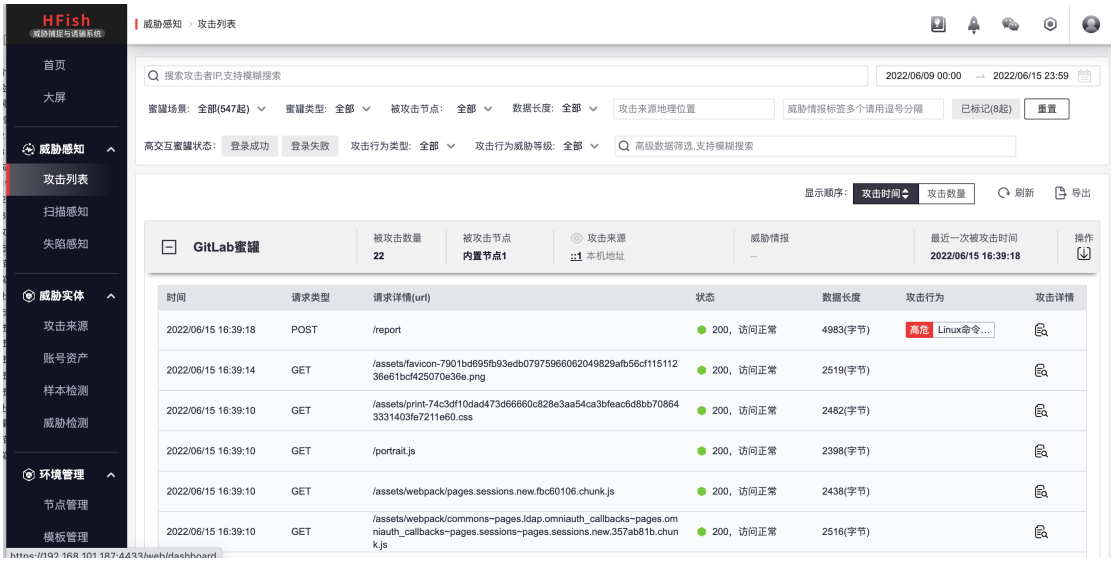

图 攻击列表威胁发现示例

另外，针对高危威胁，攻击列表提供了筛选项，可以选择只查看登录成功的攻击行为，或者有触碰威胁规则的攻击行为。

3.2 扫描感知

该页面用于展示 HFish 蜜罐节点被 TCP、UDP 和 ICMP 三种协议的全端口扫描探测行为。即使节点相关端口没有开放，HFish 仍能记录下扫描行为，此外，HFish 还会记录节点主机本身外联行为。

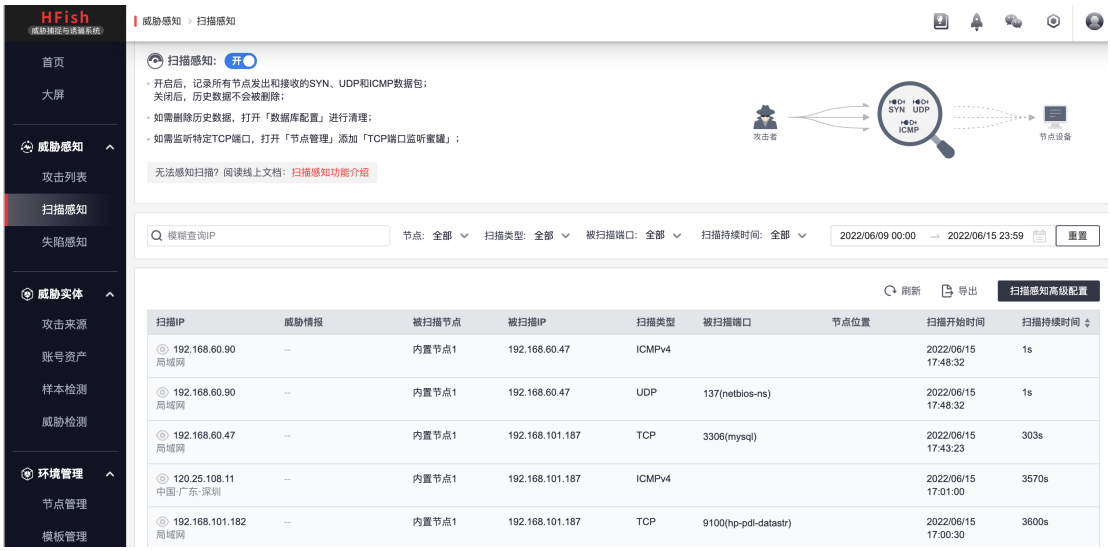

图 扫描感知告警示例

注意：Windows 节点的扫描感知依赖 WinPcap，需要手动进行下载安装！

（WinPcap 官方链接：https://www.winpcap.org/install/bin/WinPcap_4_1_3.exe）

3.3 失陷感知

HFish 的主机失陷感知依赖 HFish 诱饵体系。诱饵泛指任意伪造的高价值文

件（例如运维手册、邮件、配置文件等），用于引诱和转移攻击者视线，最终达到牵引攻击者离开真实的高价值资产并进入陷阱的目的。

诱饵的部署文档在：https://hfish.net/#/4-4-internetdecoy

图 失陷感知样例

四、外网处置建议

3.1 攻击强度封禁规则

很多红队在进行攻击之前，会先对企业资产进行探测，即"踩点"。不同于全网的傀儡机和扫描器，这样针对性探测往往会触发大量的告警。比如，对企业外部资产进行全端口扫描，以探测服务器各 IP 的资产。

所以，对于这类危害性比较大，针对性扫描单一资产的端口或者漏洞的，往往需要企业警惕并封禁较长时间。

我们结合其攻击频率，攻击样式比较多的特征，可以对其进行针对性识别和封禁。比如，对单个服务 1 分钟内发动 20 次以上，或者总计攻击次数超过 100 次的 IP，我们建议中等强度封禁。

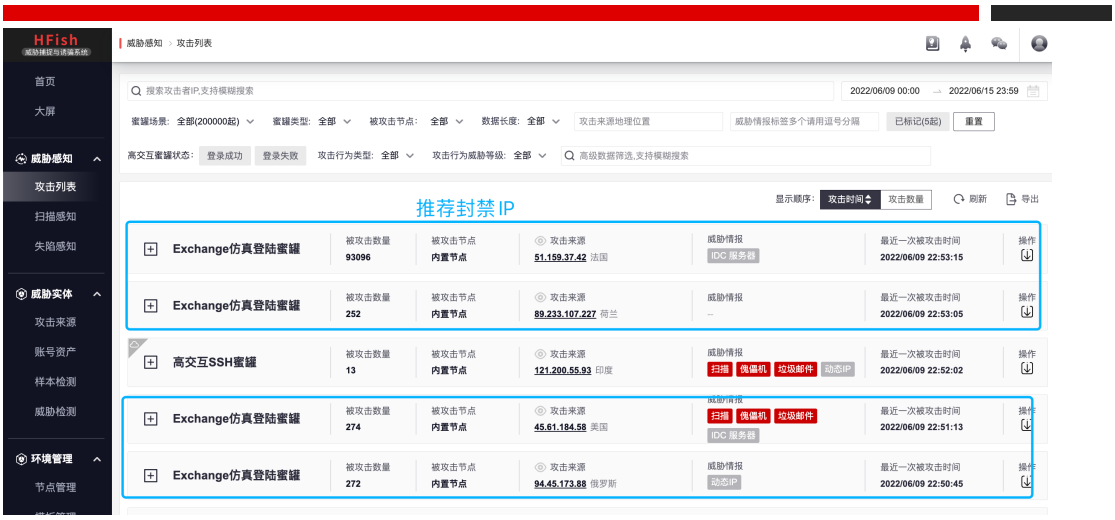

图 强度封禁示例

3.2 攻击威胁封禁规则

很多攻击情况下，对方踩点确认后，会开始使用漏洞进行攻击。这种时候，我们可以通过，HFish 的攻击行为判定，快速判定发生的行为，并快速封禁。

如果

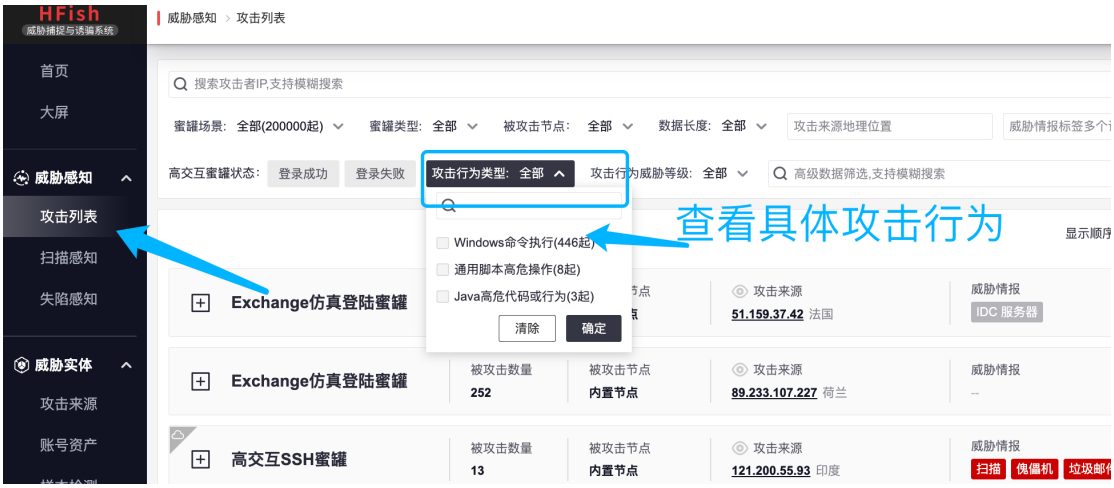

图 攻击行为查看方法

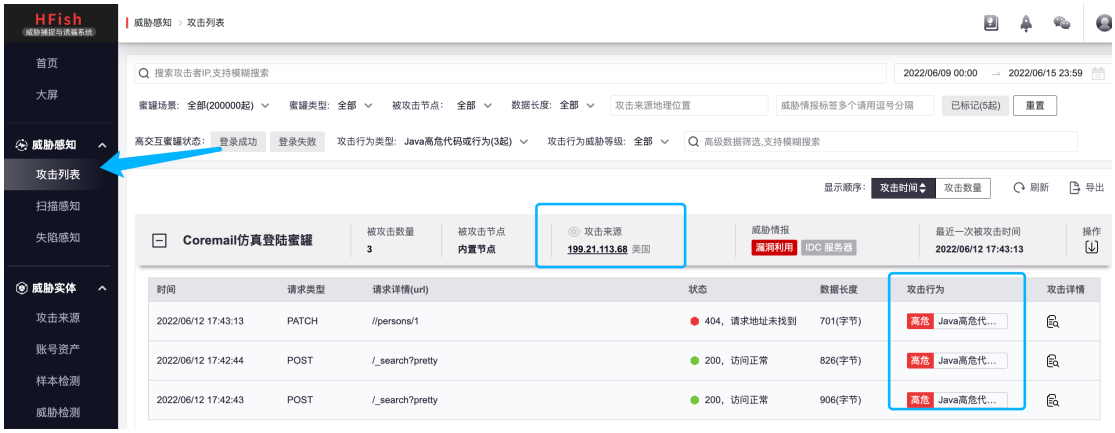

图 攻击行为查询结果

3.3 攻击 IP 情报封禁规则

联动微步情报后，在 IP 攻击时，可以快速查看到 IP 的情报属性

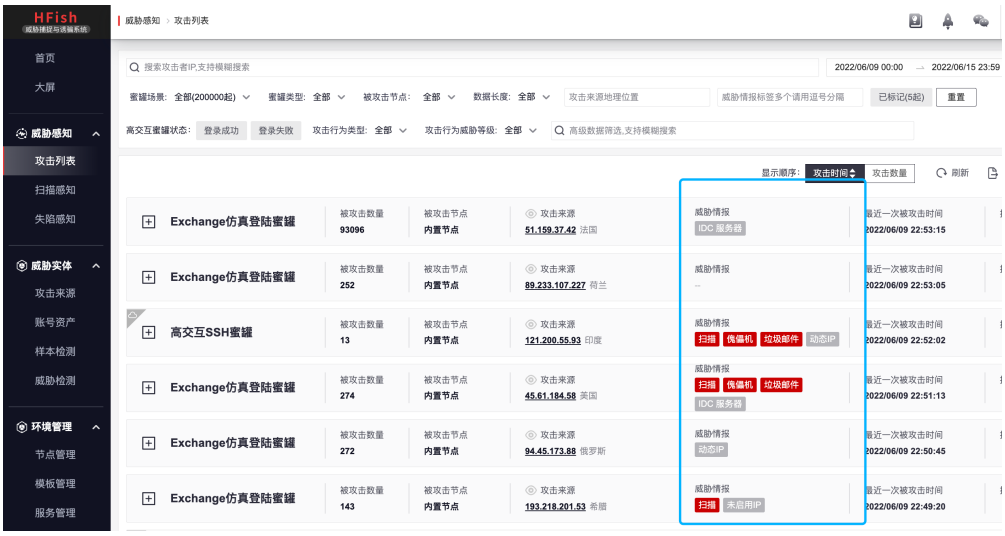

图 攻击 IP 情报查看

其中，动态 IP 中包含网关出口，移动网络 IP，小区拨号上网 IP，云主机 IP，教育网 IP 等。在微步社区可以查到这些 IP 的具体标记。

小区拨号上网 IP、企业网关 IP、教育网 IP 由于其包含较强业务属性，建议避免封禁或者封禁较短时间

移动网络 IP、往往变动很频繁，可能会存在其他被分配该 IP 的大量正常用户被误封的情况，所以不建议封禁太长时间。

云主机 IP 是攻防演练中常见的 IP 类型，同时其一般购买时间有一定时间范围，

可以对其设定时间动态封禁。

3.4 攻击上传样本封禁策略

基于 HFish 的高交互 SSH、Telnet 蜜罐，HFish 可以捕获到攻击者上传的样本信息，并自动在云沙箱进行分析。

对于云沙箱分析后显示恶意的文件，我们建议结合 IP 攻击记录，进行中等强度封禁。

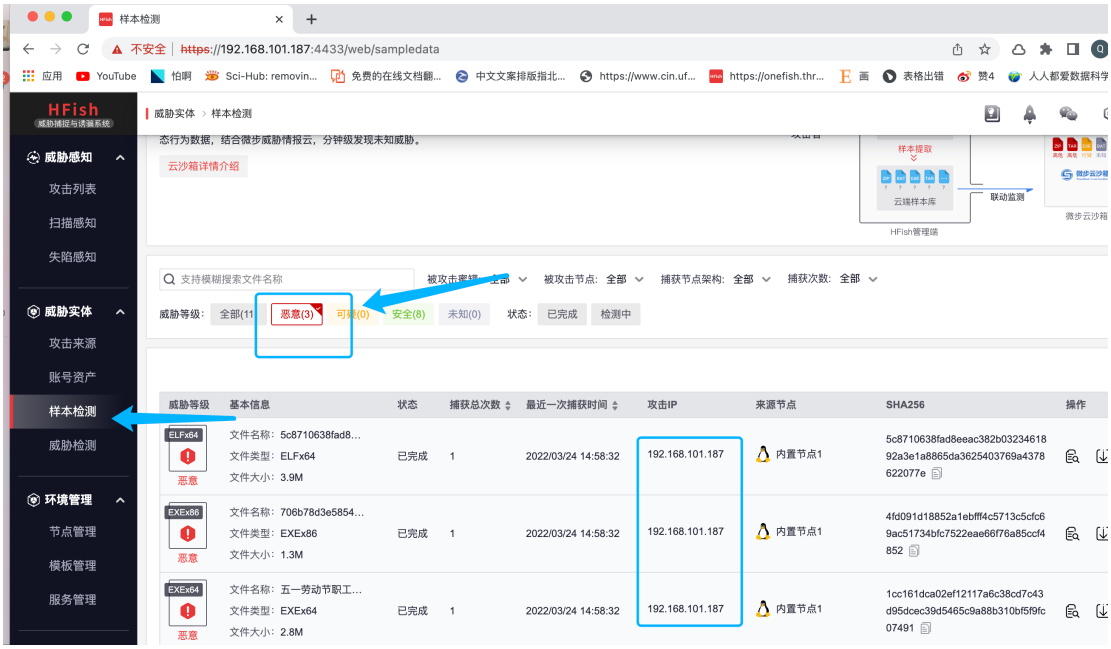

图 样本上传结果查询样例

3.5 攻击来源 IP 参考

在 HFish，【攻击来源】页面中，每个 IP 都会有一份 HFish 社区中的攻击画像。

当这个 IP 有较多的高危攻击，并且 30 天内有 15 天以上有攻击记录时，我们建议对 IP

3.6 攻击网段查看

Dashboard 界面包含攻击网段信息，其降序列出了网段攻击 IP 数量前 5 名的网段，并列出了对应的微步情报风险判定等级。我们建议攻击次数超过 100 次、微步情报为恶意的 IP，单个 C 端超过 10 个 IP 攻击时，对该 C 段提高警惕。

图 网段内 c 段 IP 处置方式

四、内网处置方式

4.1 蜜罐告警情况处理

内网的蜜罐在攻击强度和攻击数据上要远远少于外网蜜罐，在较为干净的用户环境中，我们经常会遇到的情况是，在默认 7 天的筛选下，蜜罐告警为空。

图 蜜罐告警为空示例

在这种情况下，我们有几个确认项

1. 节点的蜜罐部署是否正确，是否端口已开，能够被访问。

蜜罐可用性测试文档可参考：https://hfish.net/#/5-5-test

2. 当前部署的蜜罐是否跟区域内业务高度相似，例如区域为开发环境，可以按照环境，使用 gitlab 蜜罐、mysql 蜜罐等相仿蜜罐。HFish 在模版管理中也搭载了针对 7 种行业的 29 种不同环境模版可以一键使用。

图 HFish 行业模版示例

图 「节点管理」中一键引用 HFish 模版

3. 可自定义添加企业私有业务蜜罐

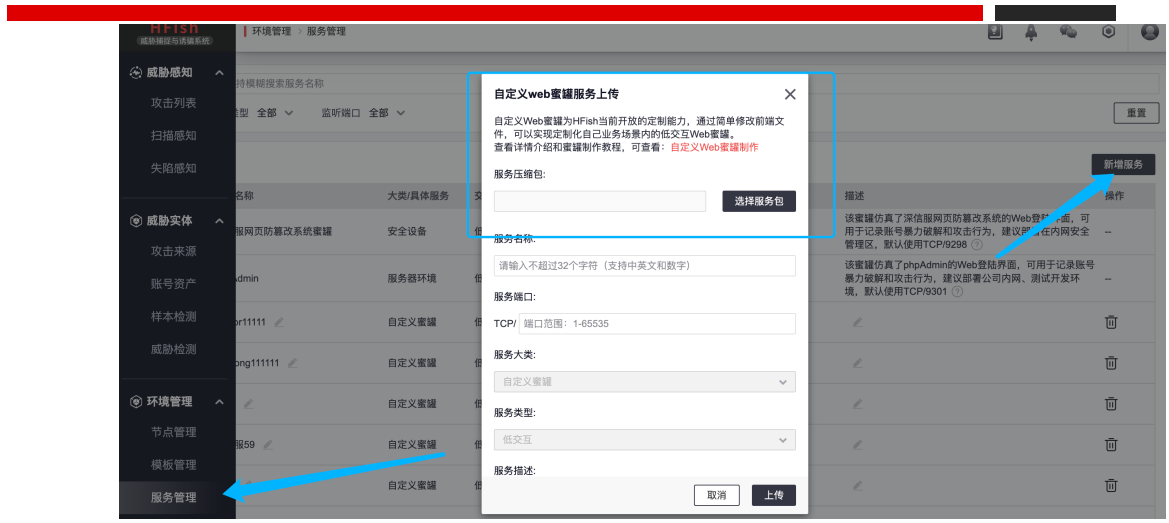

图 「节点管理」中一键引用 HFish 模版

4.2 扫描感知告警情况处理

在扫描感知功能中，我们记录节点所有的流量记录。我们建议内网一定要开启这个功能，而当处于外网环境中时，数据量大且不针对，可以选择关闭此功能。

由于功能记录所有的数据，在最初，我们会记录包括 soc，漏扫等产品的扫描记录。在这里，我们提供扫描数据高级配置功能，可以定向过滤部分 IP 和端口的扫描记录，方便运维人员排查。

图 扫描数据排查处理

4.3 失陷感知告警情况处理

HFish 的主机失陷感知依赖 HFish 诱饵体系。诱饵泛指任意伪造的高价值文

件（例如运维手册、邮件、配置文件等），用于引诱和转移攻击者视线，最终达到牵引攻击者离开真实的高价值资产并进入陷阱的目的。

诱饵的部署文档在：https://hfish.net/#/4-4-internetdecoy

如果一旦失陷感知页面，有任何的已失陷报警，我们强烈建议作为第一等级排查

1. 确认机器主人，联系是否有异常操作

2. 上机排查

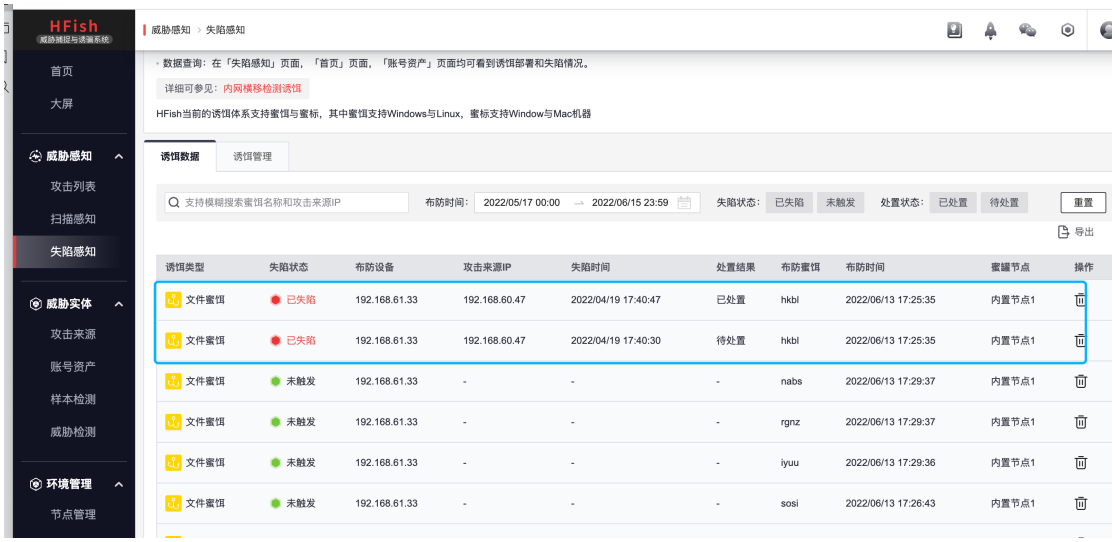

图 诱饵失陷告警内容

微步在线致力于做企业客户的威胁发现和响应专家，是2017、2019年连续两次成为唯一入选Gartner《全球威胁情报市场指南》的中国公司。微步在线提供以威胁情报为核心的安全能力，结合大数据、可视化态势感知等技术，为客户提供及时、准确、可以指导行动的威胁情报，用来对网络攻击进行预警、防御、检测以及溯源分析等。其独特的基于大数据分析的安全技术和服务能够帮助您准确、快速、低成本地实现全面的威胁监测及检测，同时也可作为原有安全防御体系的有力补充，抵御网络攻击。

我们的产品与服务

威胁分析平台（X.threatbook.cn）

中国首个综合性的威胁分析平台和情报分享社区。为全球安全从业人员和企业提供便利的一站式分析工具，功能包括：文件检测、可疑文件分析、域名/IP/Hash/URL等的安全分析、可视化分析，用以进行事件鉴别、威胁程度分析、威胁影响分析、关联及溯源分析等。为用户间进行威胁情报分享，包括样本、黑客资源、攻击手法、线索、事件等，提供免费的互动、交流环境。此外，还为企业用户提供安全运营工具、外部资产监控、行业情报等企业级服务。

威胁感知平台（Threat Detection Platform, TDP）

威胁感知平台是基于微步在线高可信威胁情报为内核的全流量检测系统。帮助决策者对系统整体安全态势全面评估，快速感知系统的安全情况等级；帮助安全运营人员聚焦真实威胁，精准定位，提供自动化处置，有效完成安全事件处置闭环。

本地威胁情报管理平台（Threat Intelligence Platform, TIP）

本地威胁情报管理平台是部署在用户本地的威胁情报管理、生产和共享中心，装载微步高可信情报数据。在配备本地超高性能检测API的同时还帮助客户进行多源异构情报的全生命周期管理；支持本地情报生产，有效防御未知攻击；赋能SoC/SIEM、防火墙、WAF等传统安防设备新的威胁能力。

OneDNS安全DNS服务（OneDNS Cloud）

基于DNS协议的安全云平台，提供SaaS化的DNS解析和管控服务。实时拦截网络设备与恶意地址间的通信，避免后续攻击行动的发生。安全管理团队可以在后台灵活配置策略，对进行内容访问控制和上网行为管理。SaaS化产品形态适配各类IT架构，使企业总部、分支机构、漫游设备和云端应用获得统一的安全防护。

检测与应急响应服务（Managed Detection and Response, MDR）

提供威胁巡检、应急响应、重保驻场、专家咨询、高级情报订阅、外部资产监控等安全相关服务。由资深安全专家提供支持，对企业内外部威胁及时发现、告警、处置、响应，并对攻击者进行画像分析与溯源分析。针对主流威胁、重大安全事件、高危APT等事件进行深度分析。提供预警、防范、处置及修复建议。针对金融、能源、政府等重点行业威胁情报及安全事件提炼分析，提供处置及应对的最佳实践，帮助提升企业安全水平。

北京微步在线科技有限公司

www.threatbook.cn

电话：010-57017961
邮箱：contactus@threatbook.cn
地址：北京市海淀区苏州街49-3号3层