HFish v2.7

威胁诱捕与诱骗系统

技术白皮书

目录

一、 产品简介

HFish 是一款基于 Golang 语言开发的跨平台蜜罐框架系统，同时支持 Linux 和 Windows 环境，可以模拟 40 种不同类型的蜜罐服务，包括：HTTPs、HTTP 代理、SSH、Telnet、FTP、TFTP、VNC、MySQL、Redis、MemCache、ElasticSearch、暗网和不同行业的 web 模拟服务。

HFish 被设计用于部署在复杂的企业内外部环境，支持分布式集群，多路 syslog、邮件和钉钉/飞书/企业微信告警输出，支持与微步在线云端 API 情报以及本地情报管理平台（TIP）对接。

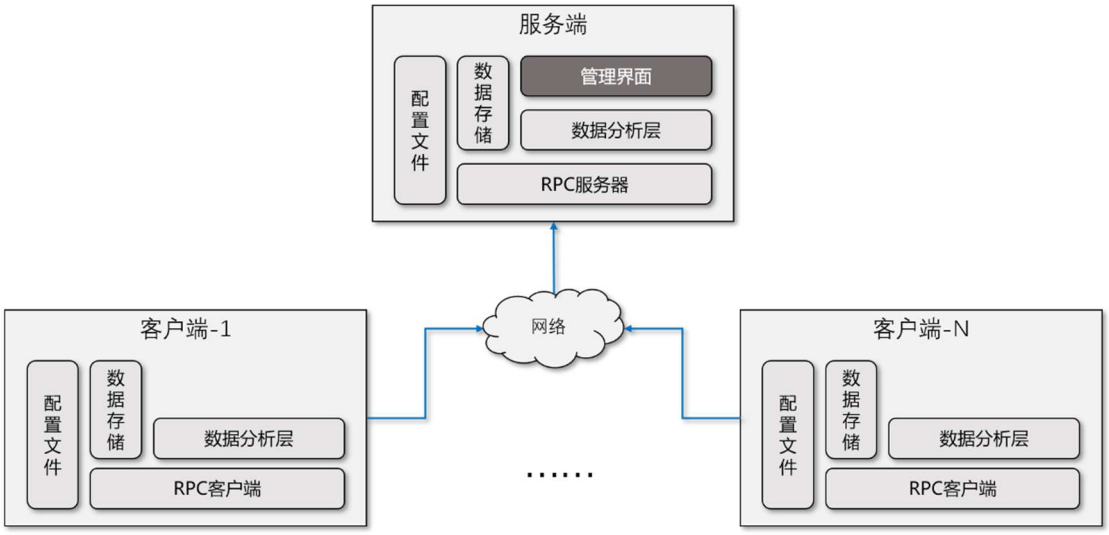
该系统可广泛适用于金融、互联网、能源、政府、制造等包含核心敏感数据的企事业单位，可部署在互联网生产区用于未知威胁检测、威胁情报生产和红蓝对抗追踪溯源场景，也可部署于内网办公区用于失陷检测和横向移动场景，能够有效帮助用户感知真实威胁、刻画攻击画像、指导安全响应、落地处置流程，最终达到“知己知彼”的网络安全防御目的，更好的进行网络风险控制。

二、 架构介绍

HFish 使用典型的 C/S 架构进行构建，单机模式下服务端（Server）和客户端（Client）同时部署在一台主机，集群模式下，服务端和客户端分离部署在不同机器上，各自通过配置文件决定节点在集群中的身份。

需要注意，与传统蜜罐产品不同的是，HFish 客户端具备完整的蜜罐服务响应能力，部署成功后，每个 HFish 客户端将独立面对攻击者攻击行为，并将攻击信息回传到服务端进行统一分析。HFish 集群架构将蜜罐服务响应和数据统计计算压力合理的分布到不同节点，特别适用于超大规模和高强度攻击背景环境内部署。

整体架构简图如下：



图：蜜罐架构简图

三、 核心功能

3.1 完备的企业环境高仿真蜜罐

HFish 内置 5 大类共计 40 种类型的蜜罐服务，同时支持高交互和低交互，用户可以根据实际需求部署在不同区域，蜜罐服务分类分别为：

大类	服务名称
基础服务	提供 SSH、TFP、HTTP、TFTP、Telnet、VNC 共六种服务。
Web 服务	提供共 29 种 web 页面的仿真服务，包括 WordPress、通用 OA、政务 OA 等。
端口监听	提供 TCP 端口监听服务
数据库服务	提供 MYSQL、REDIS、Elasticsearch、Memcache 共四种服务。
自定义服务	提供 CUSTOM 服务，可对接其他蜜罐。

3.2 适合企业环境的闪电式部署能力

HFish 是使用 Golang 语言开发的跨平台蜜罐系统，可以直接复制可执行文件到 Windows、Linux 环境执行即可完成部署，使用完毕杀死进程后直接删除目录即可完成卸载。

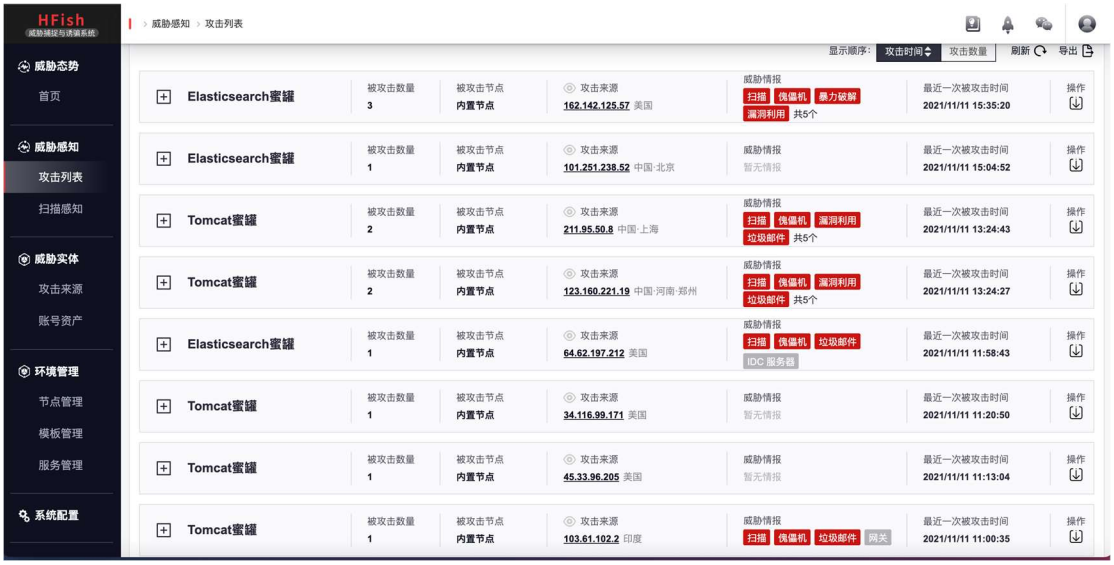
HFish 运行过程中，可实现开机自启动和宕机自启动，维持系统长时间稳定运行。

3.3 消费和生产威胁情报

HFish 已经实现对接微步在线云端威胁情报 API 和本地威胁情报管理平台（商业产品，简称 TIP），实现在 HFish 界面自动展示攻击来源地址的相关威胁情报数据。

通过合理部署，HFish 可以自动收集攻击者可指标化信息用于后续威胁检测，包括但不限于攻击者来源地址、攻击特征（木马样本、已泄露的账号密码）和资产信息（远程控制端地址、投递邮箱来源地址），并通过统计分析捕获信息，用于内部巡查和自检，早于攻击者修复隐患

图：与微步本地威胁情报平台对接实时生产私有情报



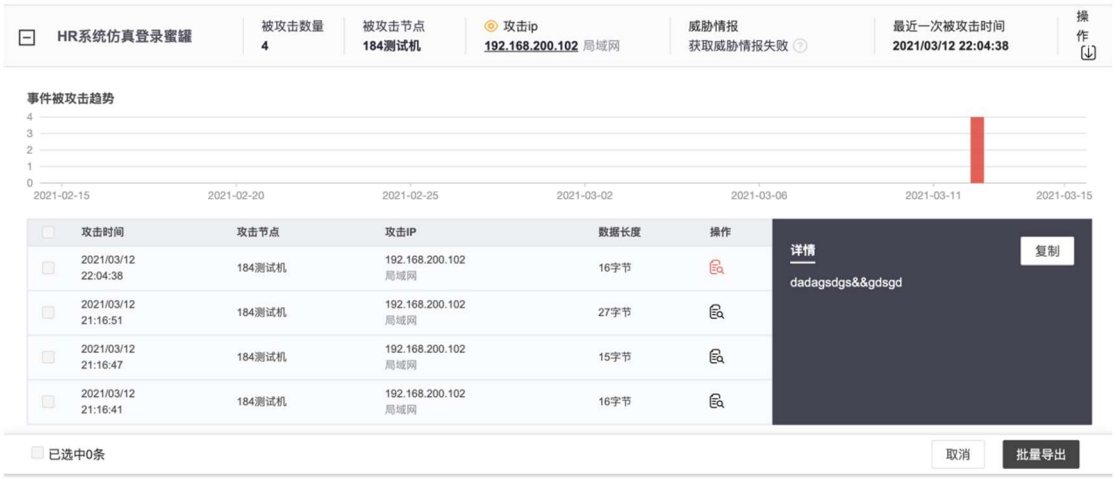
图：与微步本地威胁情报平台对接后，HFish 显示攻击 IP 情报

四、 典型场景

4.1 外网未知威胁感知

该场景的目的是尽量多的感知来自互联网的真实威胁以及涉及用户但暂时未知的威胁，例如攻击者针对我方使用的研发框架挖掘的定向攻击行为。

该场景下，蜜罐应尽量与真实生产环境部署在同一片连续的网络地址区域，并模拟仿真实际业务系统页面，但蜜罐所使用网络地址应与用户内网逻辑隔离以完全确保安全。



图：模拟 HR 系统感知到的真实威胁

案例：

某工业互联网用户通过在互联网区域部署 HFish 蜜罐，并模拟其 Web 业务系统，收集被访问 URL 加入扫描器在测试环境重放，以发现可导致系统异常的可疑行为。

4.2 内网失陷横向移动感知

该场景的目的是尽量快的感知内部失陷主机和内部未授权横向访问。

该场景下，蜜罐应该尽量均匀的部署在内部生产、测试环境，通过感知被访问情况，感知企业内部网络扫描、攻击和探测行为，并进一步发起对内部来源网络地址主机的人工或自动排查，尽快发现内部已失陷主机。

图：内网横向移动失陷感知

案例：

某金融用户在企业内部网络多个网段均匀部署 HFish，通过构造低交互蜜罐服务，实时监听并收集主动连接的内部来源地址和发送内容，通过 syslog 汇总告警到态势感知形成工单，同时邮件通告运维团队。

4.3 红蓝对抗溯源分析

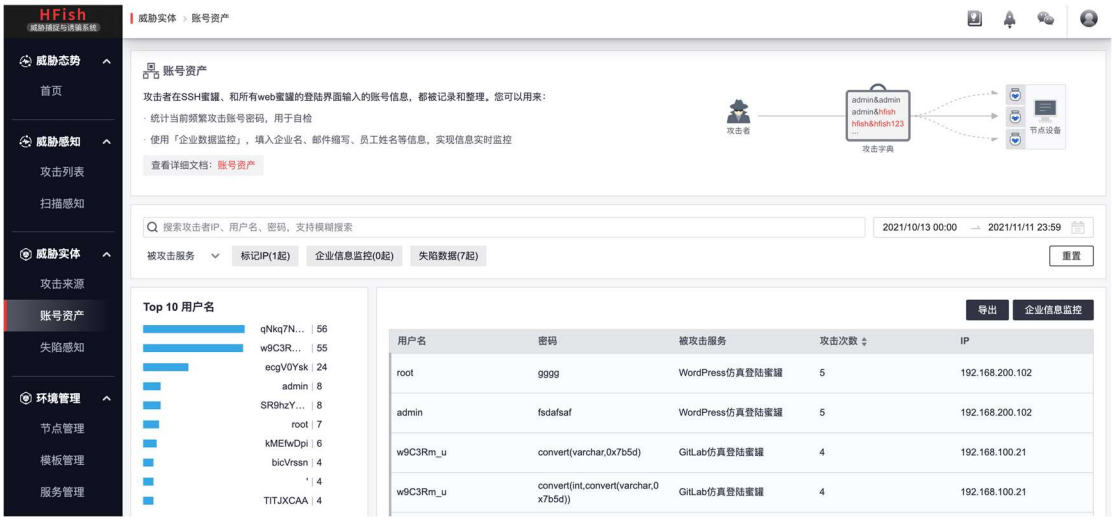
该场景的目的是尽快感知红队攻击行为，提供特殊诱饵文件引导红队下载并执行，获取红队真实 IP、微信账号、邮件地址或桌面截图等证据，以达到溯源加分效果。该方案还可在非对抗演习时长期使用，用于积累留存潜在有威胁能力的攻击者资料，便于未来面临真实攻击可直接调取攻击者档案，而无需临时溯源。

该场景下，蜜罐应该同时部署在内外网敏感主机周边网络地址，并尽量复制真实生产系统或建立看上去有价值的子域名吸引红队，例如模拟外网后台管理登录页面、外网邮件登录页面、内网运维管理系统或 Windows 域控、跳板机管理平台等。

4.4 本地威胁情报生产

该场景的目的是将蜜罐系统转化为私有威胁情报生产节点，尽量多的获得攻击者使用的可指标化信息，包括攻击者来源地址、攻击特征（木马样本、已泄露的账号密码）和资产信息（远程控制端地址、投递邮箱来源地址），并通过统计分析捕获信息，用于内部巡查和自检，早于攻击者修复隐患。

该场景下，蜜罐应尽量与真实生产环境部署在同一片连续的网络地址区域，但蜜罐所使用网络地址应与用户内网逻辑隔离以完全确保安全。



图：蜜罐使用捕获的账号密码信息

案例：

某互联网用户在互联网区域网段部署 HFish，通过构建 SSH 和伪装 Web 后台登录地址蜜罐服务自动收集攻击者使用的账号密码、C2 地址和木马样本用于：

- 检测内部员工是否正在使用，如果有，邮件通知修改；
- 将密码设置为黑名单，禁止员工后续使用；
- 将密码设置为检测指标，在代码白盒测试和上线扫描中使用；
- 重点关注已泄露的账号，对于真实存在的高价值账号实施两步验证；
- 在网络边界检测哪些主机主动连接 C2 地址，发现失陷事件；
- 通过终端管控系统下发木马哈希，排查内部主机进程和启动项；

通过以上措施，将感知到的外部威胁转化为全自动的本地威胁情报生产和检测手段，行而有效的动态强化落地安全策略，本地情报生产通常还要搭配本地情报管理平台进行威胁情报全生命周期管理。

4.5 定制企业蜜饵，进行失陷感知

HFish 可进行任意伪造的高价值文件（例如企业运维手册、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。

该场景的目的是精确定位失陷，HFish 下发的每个蜜饵都是唯一的，攻击者入侵用户主机后，如果盗取蜜饵文件中的数据并从任意主机发起攻击，防守者仍能知道失陷源头在哪里。该场景下，蜜饵适合部署在任何主机和场景中，例如作为附件通过邮件发送（检测邮件是否被盗）、在攻防演练期间上传到百度网盘或 github 上混淆攻击者视线、压缩改名成 backup.zip 放置在 Web 目录下守株待兔等待攻击者扫描器上钩等。

图：失陷感知部分，可精准呈现失陷全流程

案例：

某互用户在本地生产网部署 HFish，构建了有企业信息和符合生产网环境的蜜饵文件，并且下发到了所有的服务器上，完成

- 对所有业务主机的蜜饵防御，进行主机失陷情况监听
- 蜜饵中配置云蜜网信息，转移攻击目标至云端环境

通过以上措施，在内网的终端和服务器上增加失陷监听，不影响真实业务，不引起任何系统负担，精准感知主机失陷情况。同时，通过蜜饵，牵引攻击者的视线至云端蜜网，实现对本地业务的保护。

五、 部署要求

HFish 是一款基于 Golang 语言开发的跨平台蜜罐框架平台，可部署在 Linux、Windows 操作系统，支持 386、x86/64 架构。

HFish 服务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：

	HFish 管理端		HFish 客户端	
	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	1 G	4 G
硬盘	50G	500G	20G	50G