知道创宇
KNOWNSEC.COM

创宇蜜罐

威胁诱捕与溯源系统白皮书v1.5

（文档编号：MG-SS-2021-001）

北京知道创宇信息技术股份有限公司

2021-01-20

文档说明

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属北京知道创宇信息技术股份有限公司（以下简称“知道创宇”）所有，受到有关产权及版权法保护。任何个人、机构未经知道创宇的书面授权许可，不得以任何方式复制或引用本文件的任何片断。

创宇蜜罐威胁诱捕与溯源系统白皮书

目录

1. 企业信息安全现状

1.1. 网络安全形势严峻

- **网络安全事件**

新型冠状病毒肺炎（COVID-19）的疫情贯穿了2020年，线上办公和在线教育的兴起，也带来了安全攻防重心的转移。英国2020年网络安全年报就指出，英国政府通讯部下辖部门——国家网络安全中心——在2020年先后处理超过200次与冠状病毒相关的网络事件，几乎占上报事件总数的三分之一。

- **数据泄露**

2020年数据泄漏事件依旧呈现出原因多样性的特点，有公民个人信息的泄漏、大型网站的数据泄漏、第三方导致的数据泄漏，也有勒索软件组织泄漏的数据。除了公民个人信息被泄漏外，Xbox和Windows NT 3.5源代码也被泄漏到网上，由于Windows系统长期闭源，研究者们可以根据本次泄漏的内容了解Windows系统的底层实现原理。

- **勒索软件**

大部分被识别检测到的勒索软件往往会采取广撒网的方式进行传播，通过感染到的公网设备横向移动进而感染内网主机。在疫情之下，医院也成为了部分别有用心者的攻击目标之一，这可能会间接危及人民群众的生命健康安全。

2020 年，企业信息安全水深火热。

那些本应该在企业内网安全存储的数据却被黑客拿来公开交易，那些纯内网的核心终端居然会感染上勒索病毒导致业务停滞。

1.2. 威胁难以识别溯源

- **复杂攻击无法对抗**

网络攻击变得越来越复杂，并以越来越高的频率和效率渗透到网络中，内部人员很难立即发现威胁存在。由于员工分布在不同的地理位置，企业几乎不能保证每个员工、承包商和访问网络的第三方供应商凭证的完整性，这种情况会带来极大的安全风险。

- **僵尸网络无法感知**

僵尸网络是一种高度复杂的网络犯罪形态，由攻击者创建并对受害者电脑进行反复感染。僵尸程序会寻找易受攻击、不受保护的计算机进行感染。攻击者通过扫描网络来确定将要攻击的最佳目标数据源，这个数据源可以来自网络的任何地方。获取数据源后，攻击者从已感染的端点窃取缓存的用户凭据，伪装成该感染点，进行持续性攻击。近年来，僵尸网络+蠕虫病毒组合攻击的方式越来越常见，让网络威胁的复杂度进一步提升。

- **未知攻击无法监测**

传统设备一般仅能根据特征码判断攻击行为，0day漏洞攻击无法识别，这些未公开的漏洞被攻击者利用，会对计算机应用程序、数据、额外的计算机或整个网络造成不利影响。

- **攻击路径无法追溯**

入侵者来无影去无踪，隐藏入侵痕迹，整个过程难以发现。事后难以追踪溯源，被动且无法取证。

那么，面对网络安全威胁，我们该如何应对？

没有什么秘密武器可以一劳永逸。应当踏踏实实：事前做好防范，事后及时处理。

我们都不会享受去做事后的处理。所以，事前做好防范就变得尤为重要。

而创宇蜜罐，正是事前防范工作中的利器，将被动防御变为主动防御。

2. 创宇蜜罐将被动变主动

2.1. 产品概述

创宇蜜罐是利用网络空间欺骗技术，为倍受黑客攻击的高危行业客户提供应对高级威胁的诱捕与溯源系统。通过部署轻量级客户端，或配置迷惑性高的子域名，能有效地诱骗攻击进入预置蜜罐陷阱隔离，从而延缓攻击，保护真实资产安全，并帮助用户追踪溯源，定位攻击者自然人身份，提升主动防御能力，让安全防御工作由被动变主动。

创宇蜜罐可为企业提供被黑告警、隔离防御、攻击溯源、应急响应服务，可覆盖公有云、私有云、混合云、物理机、虚拟机等多业务环境。

通过在攻击者必经之路上构造陷阱，混淆其攻击目标，实时告警黑客的内网入侵行为，将其诱骗隔离以延缓攻击，并帮助用户进行追踪溯源、安全加固，从而保护企业核心信息资产安全。

欺骗防御技术原理：

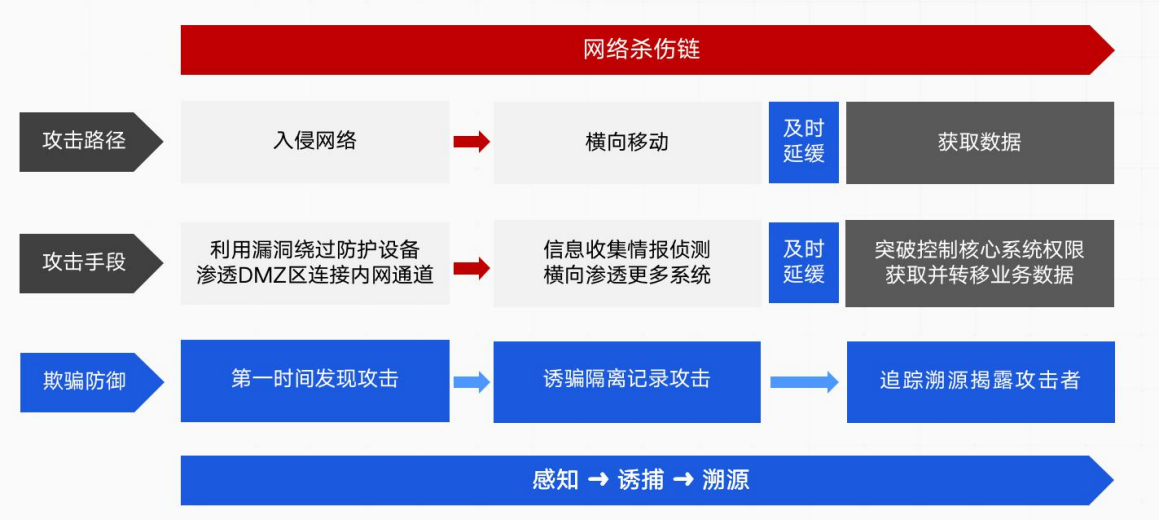

图 1. 欺骗防御技术原理

2.2. 产品结构

创宇蜜罐采用基于Web的管理方式，用户使用浏览器通过SSL加密通道和系统进行交互，方便用户使用。

- **伪装监测**

配置诱捕性强的子域名或部署客户端进行流量转移，加上蜜罐的诱捕作用，给攻击者埋下陷阱。

- **监控记录**

当攻击者被诱捕时，平台发出告警并在风险大盘实时展示数据，同时记录下详细的攻击日志与入侵记录，使攻击者痕迹一览无余。

- **溯源加固**

对攻击者的入侵数据进行溯源形成攻击者画像，在画像中展示攻击源路径以及指纹信息，生成威胁态势报告，全方面地了解企业存在的安全隐患点。

- **安全策略**

基于创宇自研KSP安全操作系统，进行蜜场安全隔离，设置流量限制等措施，使所有数据加密传输以保证整个产品的安全性。

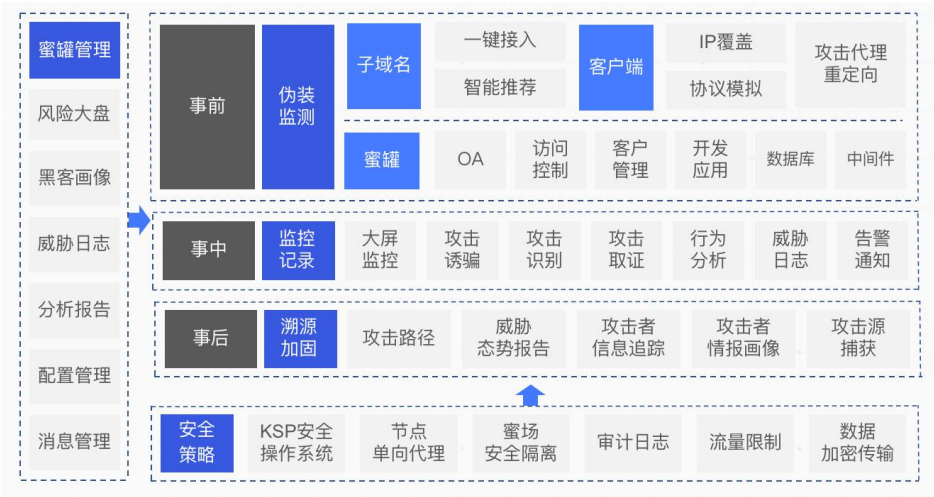

图 2. 创宇蜜罐产品结构

2.3. 产品功能

2.3.1. 高交互蜜罐

高交互蜜罐是创宇蜜罐的核心能力之一，是其成功实现攻击诱导、保护真实资产的重要基础。高交互蜜罐不仅具备完整操作系统的正常交互响应，在此基础上部署的仿真业务系统及漏洞，更让蜜罐具有足够的诱惑性，同时，由于高交互蜜罐系统不应该承载真实业务，因此发现的任何流量都可认为是恶意行为，这样能大幅提升威胁发现、跟踪能力。更进一步地，通过将多个高交互蜜罐组成蜜网，让攻击者误以为进入真实业务环境，殊不知所有的行为均被一一记录和监视。

具体地，高交互蜜罐能够对以下多种类 IT 设施进行模拟：

- **网络协议与基础服务**

  例如SSH、DNS、FTP、Samba、SMTP、Rsync等等。

- **数据库与开发应用**

  例如 ElasticSearch数据库、MySQL数据库、MongoDB数据库、Redis数据库、代码托管服务、研发协同平台等。

- **业务应用**

  例如 OA、CRM、邮件系统等。

- **防火墙类**

  例如堡垒机服务、VPN客户端等。

- **自定义蜜罐**

  用户可以通过基础蜜罐 + 自定义服务内容的方式实现与自有业务高度相似的蜜罐。

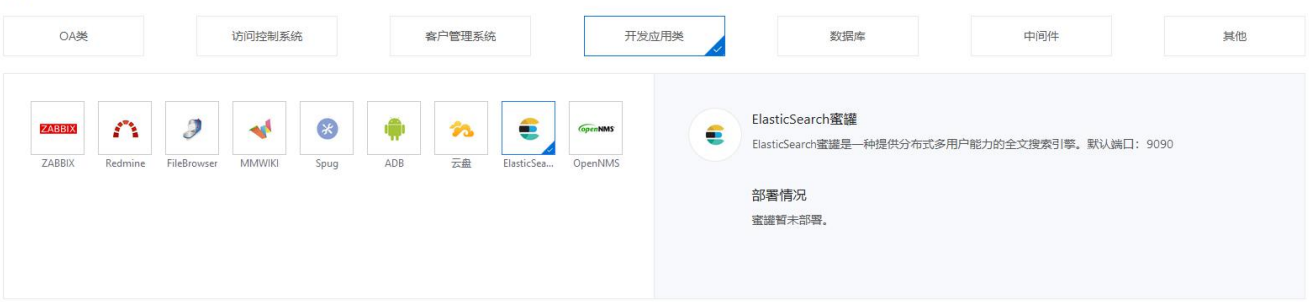

图 3. 多场景高交互蜜罐

2.3.2. 内外网路径诱骗

创宇蜜罐提供客户端与子域名两种路径诱骗的方法，分别应用于内外网不同场景。

- **内网场景**

在内网场景中，蜜罐的入口散布的越多，捕获到攻击者的概率也会更高。通过在隔离网段旁路部署客户端，利用IP覆盖将大量空闲IP分配给蜜罐服务（可以覆盖 C段、B段，甚至 A 段），结合产品提供的中继链路模式实现跨网段部署，这些 IP 地址最终都会被重定向至蜜罐环境，成为蜜罐的入口。此时内网中若存在被入侵并中毒的设备，在试图横向攻击时，蜜罐捕获到攻击的几率便会大大提高，从而快速在众多资产中定位隐藏的被感染设备。

- **外网场景**

在外网场景中，可以配置解析蜜罐系统智能推荐的具有高诱捕性的子域名，并结合部署Web类高仿真蜜罐（如：企业官网、OA系统、电商网站、论坛等）。在没有官方入口的情况下，真实访客通常不会进入诱捕子域名，而试图从旁站突破的攻击者，则更可能在扫描探测时进入诱捕子域名，从而被蜜罐捕获。

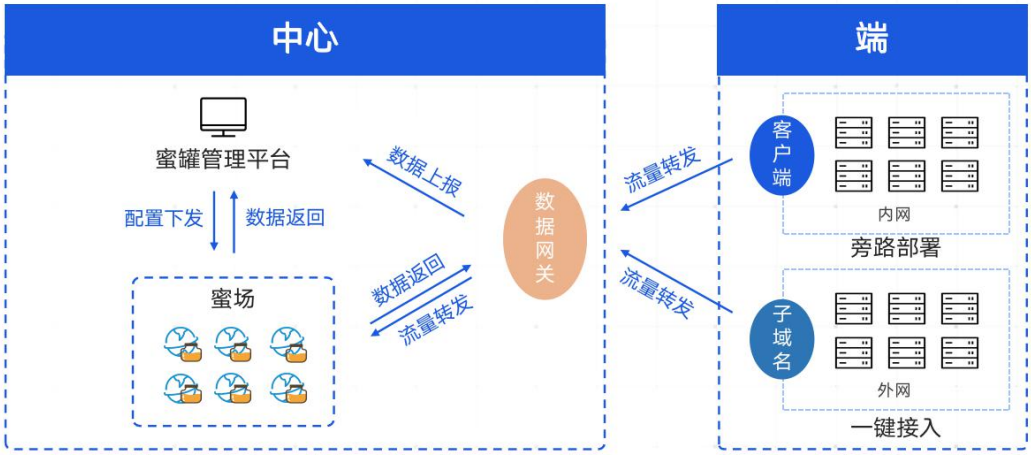

图 4. 内外网路径诱骗

2.3.3. 实时风险态势

风险大盘视角全面动态展示网络资产保护状态，分析威胁监测数据并生成可视化图表，蜜罐状态与攻击数据一览无余。

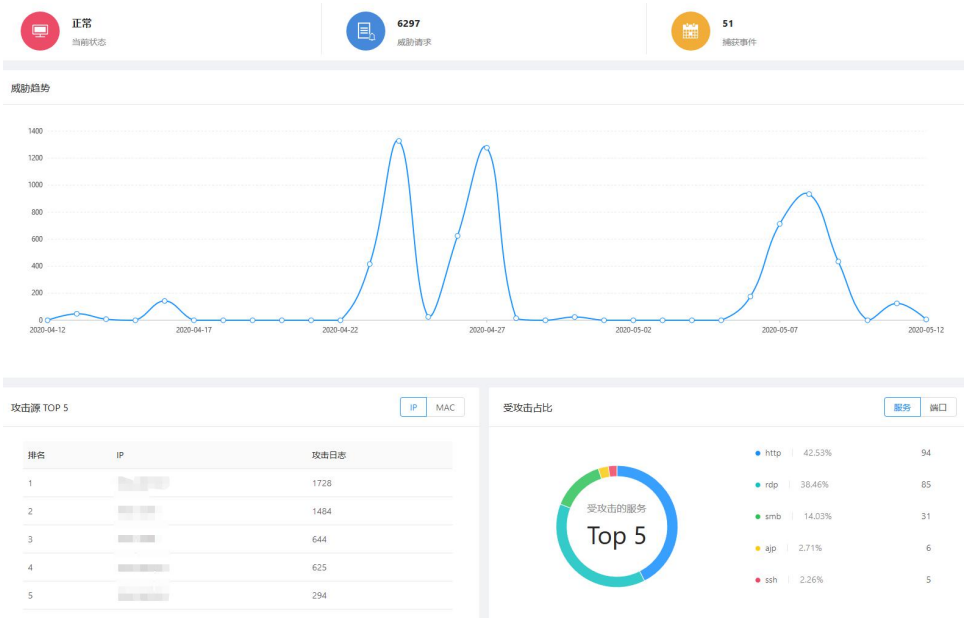

图 5. 威胁态势

2.3.4. 威胁记录监测

安全运维人员在收到告警消息后，可以登入创宇蜜罐管理系统，查看此次威胁事件

的详情。创宇蜜罐尽可能丰富地收集威胁事件日志，用户可下载威胁事件的详细日志数据包用于分析。

对于高交互型蜜罐，比如当攻击者以 SSH 方式登入蜜罐后，创宇蜜罐将全程记录此次会话，用户也可以回放本次攻击，以视频形式观看此次攻击会话的全过程。同时蜜罐还会监听并获知攻击者可能在蜜罐中上传的文件，并且为这些遗留文件在页面上提供下载分析途径，使蜜罐系统成为大规模采集恶意样本的途径之一。

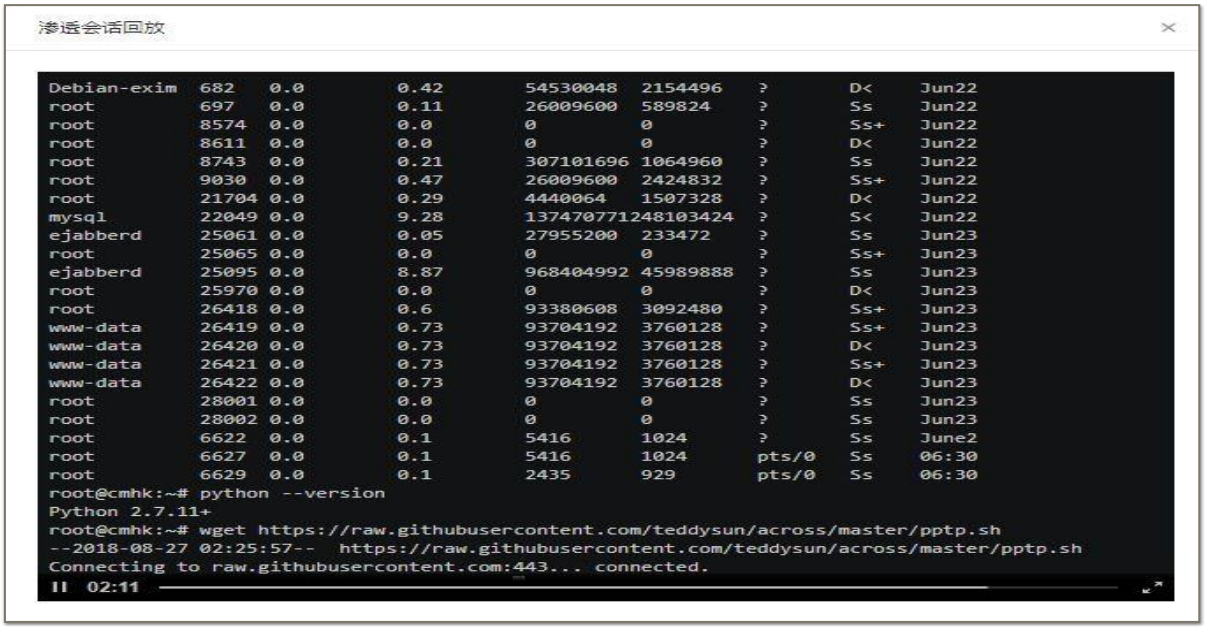

图 6. 会话回放

2.3.5. 黑客画像溯源

设陷埋点诱骗攻击者并主动追踪获取黑客的身份信息，当攻击者入侵到创宇蜜罐所设的蜜网中，创宇蜜罐数据分析中心对攻击数据进行全面分析，识别攻击行为，获取攻击者指纹信息，将攻击路径可视化，生成攻击者画像，协助客户找到攻击源。

针对单个攻击源，创宇蜜罐从多重维度对攻击者身份进行分析并结合创宇安全大脑进行立体画像绘制，包括真实 IP、虚拟身份、设备指纹等信息。

- **真实 IP**

通过漏洞利用，获取攻击者内、外网真实IP、代理IP、局域网IP。

- **设备指纹**

根据攻击者的攻击请求，配合指纹识别插件，分析出攻击者所用客户端上的特征指纹，并计算出唯一身份识别符。

- **虚拟身份**

储备大量社交网络网或APP漏洞，有效对目标的身份信息、社交关系等信息进行探测，获取目标常用网站的真实 ID、头像和账号内容等，进一步可获知其物理地址、真实姓名等有价值信息。

- **攻击手段**

借助创宇安全大脑，从国内、外全网安全大数据库中匹配攻击者的历史攻击数据，分析其攻击手法。

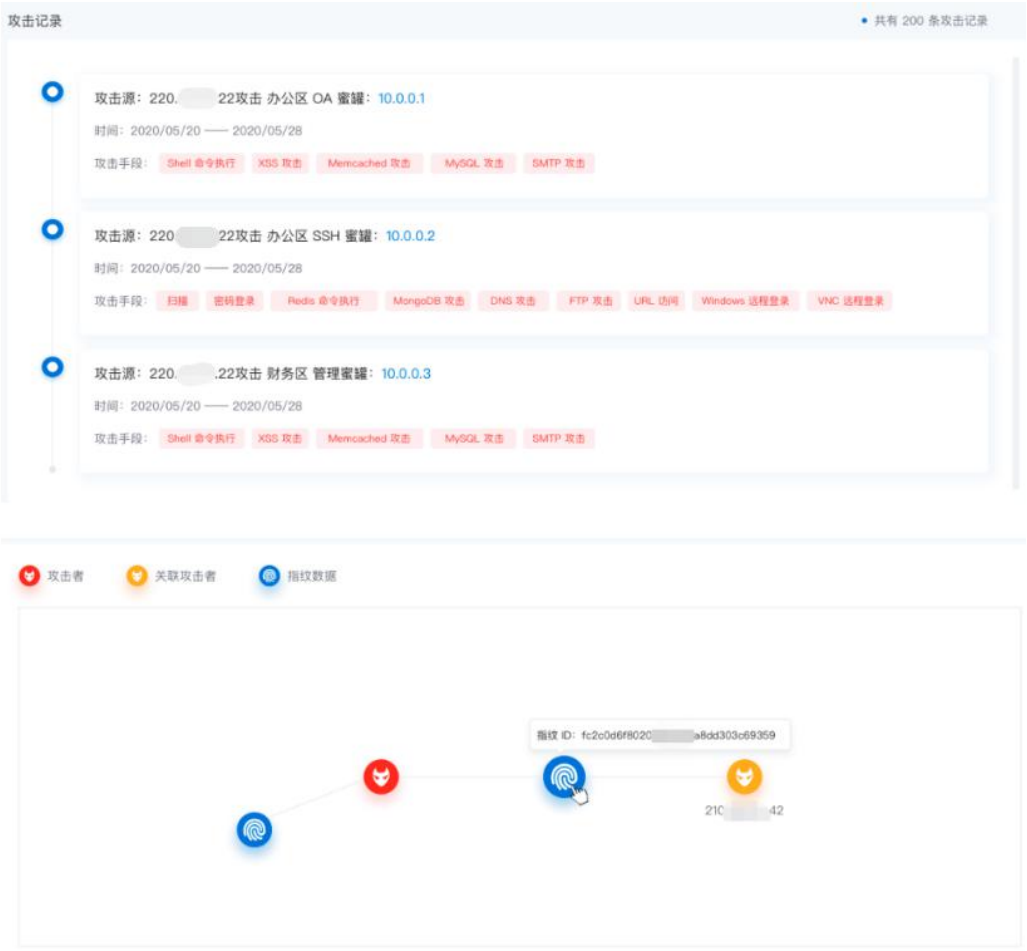

图 7. 攻击溯源

2.4. 产品特点

2.4.1. 域名一键接入云蜜罐

✧ 全网**首家云蜜罐**模式，支持子域名一键接入云端，快速部署海量蜜罐。无需额外安装部署，只需将子域名解析到云端蜜场，即可部署网站蜜罐。

✧ 云端蜜罐资源可快速调整，使得蜜罐可以根据用户的使用压力随时扩容。

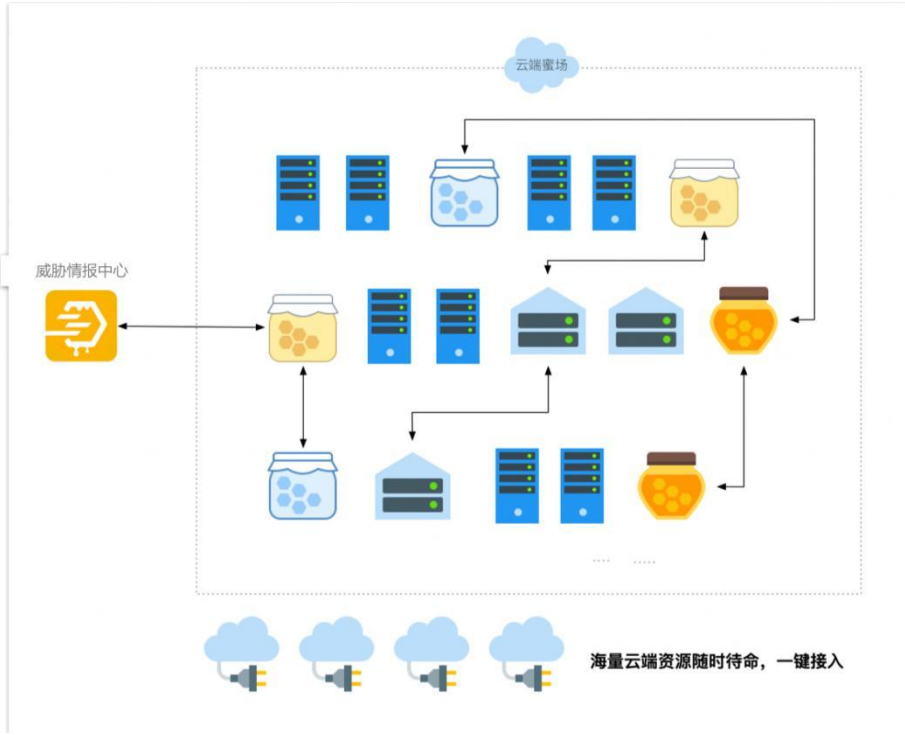

图 8. 高级仿真的云蜜罐

2.4.2. 轻量、无侵入客户端

✧ 轻量，仅包含数据转发与攻击感知的功能，使得客户端占用资源极少，十几秒即可部署成功，可在较低配置的服务器上运行。

✧ 无侵入，不需要在现有的业务服务器上安装软件，不会对现有的业务造成影响。

✧ 多网卡支持，如果您的一台服务器有多张网卡，那么一个客户端可以支持虚拟多张网卡，使得硬件资源得以最大化利用。

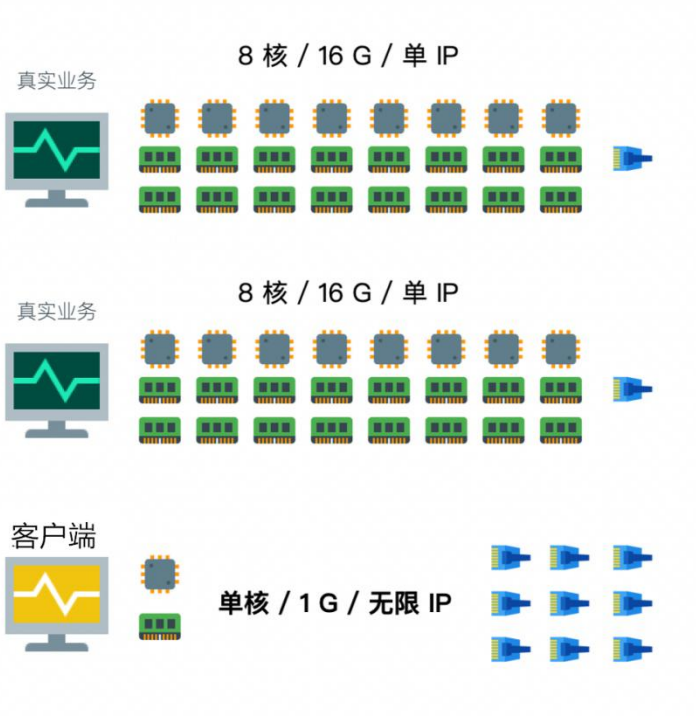

图 9. 轻量、无侵入的客户端

2.4.3. 精准告警、数据联动

支持数据推送实现消息联动，可以将蜜罐平台所记录的黑客威胁数据字段根据需要利用SYSLOG推送到其它安全可视化平台上。这样就提供了足够的威胁情报数据分析的来源日志，并且实现与其他第三方设备联动的优势。

✧ 创宇蜜罐数据处理中心可以在数据上报的第一时间发送告警事件到用户。

✧ 将晦涩难懂的数据流转换为可视化报表和易于检索、定位的攻击日志。

✧ 能够根据威胁数据生成网络安全报告，整体安全局势一目了然。

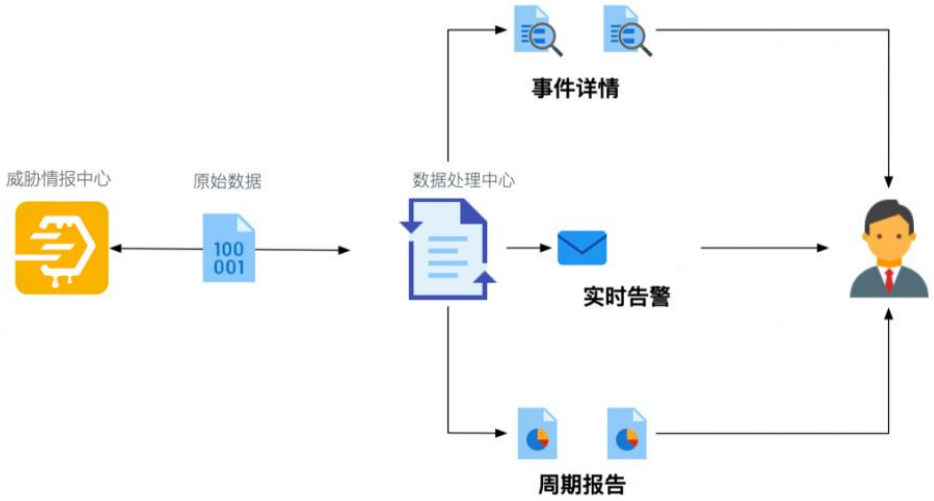

图 10. 实时精准的数据处理

告警类别	描述	推送策略
威胁事件告警	实时分析发现的威胁事件	全量推送
态势告警	根据威胁流量趋势，判定攻击峰值，进行告警	峰值敏感度
系统运行状态告警	客户端状态、服务器负载、IO、网络等异常告警	全量推送
周报、月报	生成选择时间范围内的威胁感知报告	自定义周期

2.4.4. 丰富的可视化报告

✧ 基于对威胁事件的统计分析，创宇蜜罐提供一系列的可视化图表与报告，方便安全运维人员进行态势评估与趋势分析，威胁处置建议可以为安全运维人员提供决策依据。

✧ 蜜罐系统监测到的威胁事件的走势情况，可以分析当今及未来一段时间的网络安全形势，提前加固，防患于未然。

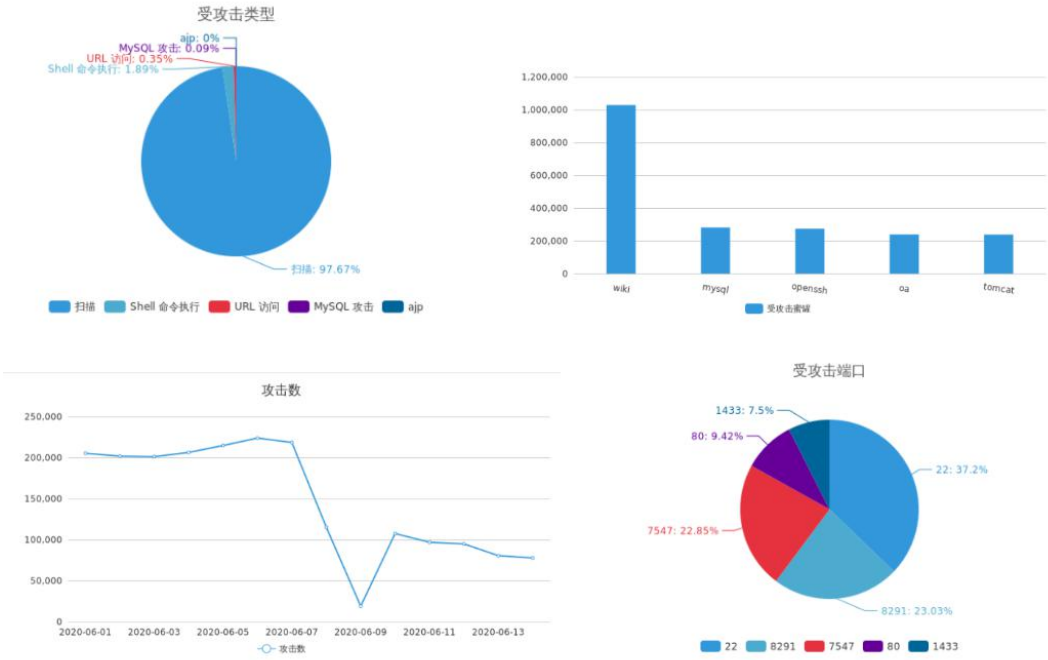

图 11. 丰富的可视化报告

2.4.5. 迭代提升捕获能力

创宇蜜罐与知道创宇 404 安全实验室、SeeBug漏洞平台密切合作，时刻关注着业界安全态势，对蜜罐内容及类型不断研究更新，能够覆盖各种功能场景，并且采用插件形式灵活迭代、提升蜜罐能力，增加蜜罐的高交互性以及数据捕获能力，最大程度吸引黑客进入、延缓攻击行为，同时有效提高反制入侵者攻击的成功率。

✧ 研究成果将不断强化创宇蜜罐的分析能力，做到敌进我进，知己知彼。

✧ 持续跟进业内最新的攻击手法、自动化病毒等，并针对性制作对应的蜜罐部署到创宇蜜罐蜜场内。

2.4.6. 高度自身安全保障

✧ 创宇蜜罐内部从网络隔离、环境隔离、流量单向控制等各个维度配置了安全防护系统，保证系统自身不被攻击者识别和破坏，以及不会被作为跳板对其它目标发起攻击。

✧ 数据加密传输，确保攻击者无法截获有用信息。

✧ 蜜场与外部网络隔离，无法由蜜场连接其他系统。

✧ 客户端旁路部署，攻击只能单向代理至蜜罐。

✧ （KVM+Docker）蜜场虚拟化+KSP安全操作系统。

2.4.7. 安全专家应急响应

在必要时刻，用户可联系创宇蜜罐团队一键接入知道创宇「紧急入侵救援服务」，安全应急专家将协助用户实施专业的入侵应急措施。

2.5. 产品部署形态

2.5.1. SaaS 版

创宇蜜罐支持SaaS版本，客户按需购买服务，节约成本。SaaS云平台自动更新，专人维护，无需额外运维管理。

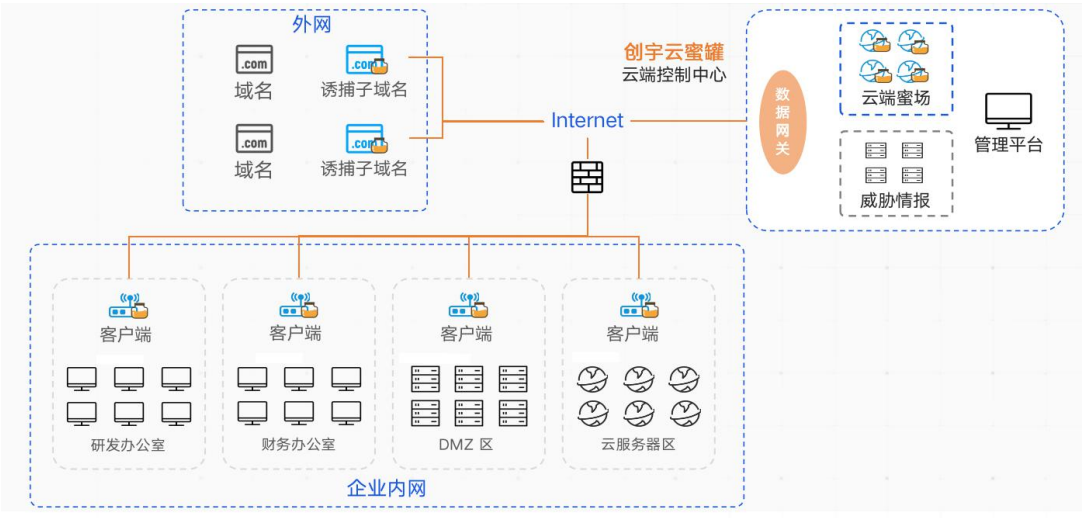

图 12. SaaS 版部署示意图

2.5.2. 私有版

创宇蜜罐同时支持私有版硬件或软件部署，硬件提供标准2U服务器，软件则支持实体机和虚拟机部署模式。

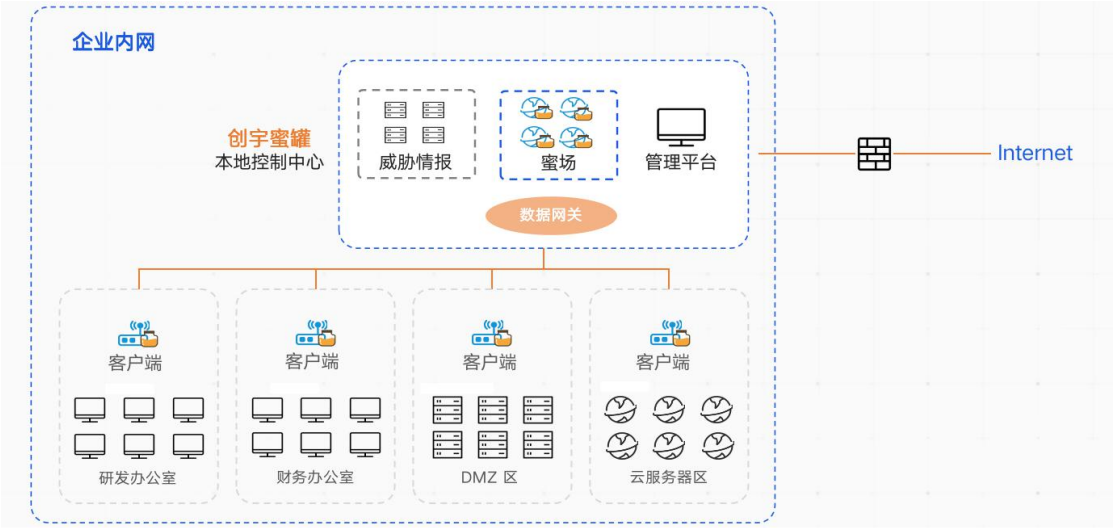

图 13. 私有版部署示意图

3. 应用案例及收益

3.1. 应用案例

3.1.1. 内网蜜罐协助电商企业及时发现内网感染勒索病毒

蜜罐产品被部署在内网中，可以及时发现内网安全事件，例如勒索病毒、误操作攻击等，保护用户真实资产安全。某电商行业公司在网络安全防护方案中配备了创宇蜜罐及创宇盾，其中创宇蜜罐为私有化部署，在内网共部署了3个客户端和8个蜜罐。

蜜罐通过仿制该公司敏感数据、仿真Web系统、模拟真实业务系统等方式，提高蜜罐的伪装程度。同时蜜罐通过部署在真实网域、使用空闲IP等方式实现路径诱骗，用蜜罐替代真实系统引诱攻击者发起攻击。部署完毕后，通过持续监测，发现3天时间里蜜罐在内网环境中截获攻击威胁请求3万余次，其中更是成功阻止了一起有针对性的勒索病毒攻击事件。

根据对威胁告警日志进行分析，攻击者对蜜罐系统访问频率极高，先是针对蜜罐发起了全端口扫描以及大量445端口的针对性扫描，利用开放端口入侵蜜罐系统，进行了非常典型的字典口令爆破攻击，在爆破成功后立即修改了账号密码，随即上传勒索病毒。

安全专家指出，该攻击疑似为感染勒索病毒的设备发起的攻击行为，经过排查，成功在内网中查到感染病毒的设备，及时阻止了攻击者利用中毒设备作为跳板，对内网的Windows主机发起横向移动攻击，彻底打消了攻击者试图获取更高访问权限及悄无声息攻破内网的企图。

勒索病毒攻击一旦成功，除攻击者外是很难进行解密的，为了恢复系统数据，被攻击者往往不得不缴纳“赎金”。而蜜罐通过网络诱捕攻击，代替原目标系统被植入勒索病毒，则起到了延缓攻击保护真实系统的作用。在这之后，通过分析蜜罐中攻击者的攻

击手段和攻击路径，进行“查缺补漏”，可以对公司系统进行有针对性的安全升级加固。

3.1.2. 省级事业单位通过蜜罐实现攻防演练溯源得分

在2020年专项安全演练中，某省级事业单位在外网部署了创宇蜜罐特有的SaaS版网站蜜罐，伪装成为单位的行政系统，还将诱惑性强的域名解析到蜜罐地址上，用来诱捕攻击者，希望将攻击者针对外网资产侦察、踩点行为进行集中分析。

在攻击者访问蜜罐时，其对蜜罐发出的访问请求中会携带自身的设备特征，而蜜罐中内置的溯源插件会对攻击者所用电脑操作系统、浏览器版本、浏览器所处时区等设备指纹数据进行抓取，也能基于浏览器特性获取到攻击者本地访问的邮箱、论坛、社交平台等互联网账号的相关信息。

该省级事业单位部署蜜罐的攻击态势和威胁告警日志中显示，蜜罐7天内共捕获威胁请求超过67万次，其中包括10多起口令爆破、1起Webshell上传，经过蜜罐威胁分析引擎可以清晰看到每一次的攻击命令。通过蜜罐详细的攻击路径数据记录和攻击行为回放分析，值守人员第一时间将发起攻击的攻击源IP上报给处置组进行封禁，同时应用数据大脑情报库进行全网溯源，得到了攻击者的完整画像，包含该攻击者历史上的攻击行为，以及其活跃的网络 ID 和真实身份、工作单位、地理位置信息等，在攻防演练中获得加分。

3.2. 用户收益

- **增强高级威胁防御能力**

有效感知威胁，能够捕获 勒索病毒、APT、0day、隐蔽信道、社交工程等高级、未知威胁。

- **诱骗攻击保护真实资产**

将攻击诱捕至蜜罐，进行隔离，为客户争取响应时间，保护真实资产不受侵害。

- **发现并加固网络薄弱环节**

事后根据对攻击过程的分析，发现网络薄弱环节，针对性的对网络加固升级。

- **提升威胁捕获响应效率**

捕获威胁第一时间告警，并自动分析威胁行为、直观展示攻击路径，提升威胁响应效率。

- **有效追踪溯源并反制攻击者**

对攻击全要素记录，取证溯源，并预设陷阱，主动获取攻击者信息，有效追踪溯源，并对攻击者实施反向控制，掌握防御主动权。

- **数据展示报表导出**

将威胁数据以风险大盘的方式实时动态显示，威胁数据支持报告导出，全面分析网络存在威胁。