欺骗诱捕技术在气象网络安全攻防对抗场景下的应用

周琰　马强*

(国家气象信息中心,北京 100081)

摘要　随着信息技术的快速发展,网络安全形势愈发严峻,气象部门通过组织网络攻防演习,以实战标准检验并提升业务安全防护体系能力。在演习中,攻击队伍对重要业务单位的真实网络及信息系统进行攻击渗透,各业务单位作为防守方开展实时监控与应急处置。由于攻防双方信息不对等,防守方采用传统防御手段经常处于被动挨打的局面。为提升网络防御能力,本文研究伪装欺骗和攻击诱捕技术在气象部门网络安全实战场景下的应用,通过采用基于蜜罐的欺骗诱捕平台,构建主动防御体系,实现对异常网络流量的监测、分析和预警,并对攻击方进行诱捕、溯源。经过实战检验,欺骗诱捕技术的应用切实提高了网络安全防御能力,保障气象业务系统稳定运行。

关键词　网络安全;欺骗诱捕;攻防对抗;流量重定向;行为分析

中图分类号:P409,TN915.08　**DOI**:10.19517/j.1671-6345.20220126　**文献标识码**:A

引言

近年来,随着网络安全形势日益严峻,来自境内外黑客组织、非法机构的活动日益增多,针对政府、金融、能源等行业单位的APT(Advanced Persistent Threat,高级持续威胁)攻击事件频繁发生[1],严重威胁国家安全,网络安全上升至国家战略层面[2]。气象部门的勒索病毒、密码破解和网页篡改等安全事件也时有发生,由国家气象信息中心监测到国家级气象网络的安全威胁告警数量从2019年的569万条增长为2022年的1560万条,安全形势越来越严峻。虽然绝大部分威胁均已被传统的安全防护手段拦截,但是仍会有少数存在安全漏洞的业务系统受到攻击,影响气象业务的整体稳定性。

国家有关部门贯彻国家网络安全战略,组织开展网络空间攻防对抗演习。通过设定演习规则,由经验丰富的安全领域技术专家组成攻击队伍,对重要业务单位的关键信息基础设施进行攻击渗透。气象部门也由网络安全专业技术人员组成防守队伍,与攻击方进行抗衡。通过模拟实战,发现防守方网络安全漏洞,促使防守方提升网络安全意识,增强防御能力,以达到提高网络安全防护水平的目的。

攻防演习设置演习指挥部、攻击方和防守方等角色,并制定相应演习规则。防守方通常会在日常安全运维工作的基础上,以实战思维进一步加强安全防护措施、提升管理组织规格、扩大威胁监控范围、完善监测与防护手段、增加安全分析频率、提高应急响应速度、提升防守能力。攻击方在不影响防守方业务系统稳定运行的前提下,对防守方信息网络系统进行渗透,实施以获取重要系统权限为最终目标的网络攻击[3-4]。攻击方通过模拟攻击,获取内网主机的访问权限,将内网主机作为跳板机[5],进行横向移动[6],在内网搜集大量信息,获取大量主机权限、核心系统权限或敏感数据后,完成攻击过程。

在实战演习中,攻守双方之间信息的不对称,成为了防守方做好网络安全防护的巨大挑战,表1列出了攻守双方资源和能力的实际对比。

国家气象信息中心信息网络安全与“信创”技术研发创新团队(NMIC-202011-05)攻关任务、国家气象信息中心科研项目结余资金课题(NMICJY202320)、国家重点研发计划项目(2016YFA0602100)资助

作者简介:周琰,女,1978年生,正高级工程师,主要从事气象网络安全,Email:zhouyan@cma.gov.cn

收稿日期:2022年3月24日;定稿日期:2022年11月4日

*通信作者,Email:maqiang@cma.gov.cn

表 1　攻守双方资源和能力对比

资源	攻击方	防守方
信息资产	分散在全网的匿名 IP 主机,可用于信息收集和攻击	公开的域名、IP 和单位信息 商业化的软件资产
情报	可利用各类工具预先获取防守方信息	攻击方发起攻击前,对攻击方一无所知
工具	①武器化的漏洞利用工具 ②定制化的远程控制工具	①商业化的网络设备 ②商业化的安全防护系统
人员	专业攻击渗透人员	①网络和应用运维人员 ②专职安全工程师
时间	不限定攻击时间	①常规 8 h 工作制 ②战时 24 h 值守
目标达成条件	①0day 利用 ②钓鱼、鱼叉目标中招 ③不安全配置 ④其他	①24 h 全方位监控体系 ②人员严格遵守安全要求 ③严密的安全配置和漏洞管理 ④其他

气象部门是关系国计民生的重要公益性部门,履行公共气象服务职能,具有大量通过互联网提供的气象预报、气候预测、宣传科普和云会商[7]等资源,同时也支撑台风登陆[8]、暴雨灾害[9]、重大活动等气象服务保障中的决策气象服务[10]。由于气象部门国省市县垂直体制四级连通一张网,且互联网暴露面众多,极易被利用进行攻击渗透,使得防守方处于非常不利的局面。如果真实发生有组织、针对性强的大规模网络攻击,势必严重影响气象业务安全,损害社会秩序和公共利益。

气象部门近年来持续加强网络安全技术防护和服务能力,初步建立了网络安全基础防护和安全事件监测系统。但随着内、外部网络安全形势变化和新技术的不断发展,传统的技术防护手段已经无法完全满足业务发展对网络安全的需求。因此,气象部门作为防守方亟需改进技防手段,在攻防对抗场景下利用气象数据共享、气象信息公开等特点[11],引入欺骗诱捕等主动防御技术完善网络安全防护体系,提升安全服务能力,在攻防对抗中占据主导地位,与攻击方进行有效对抗,扰乱其视线、延缓其攻击进程,进一步对其进行追踪溯源[12-13]。

本文研究了伪装欺骗和攻击诱捕技术在攻防对抗场景中的应用,从实战角度阐述该技术在增强防守方防御能力、保护气象业务安全方面的价值。

1　欺骗诱捕技术

1.1　概念

实战演习中,防守方的各类域名、IP 地址及重要业务系统等网络资产信息相对公开,而攻击方信息相对保密。防守方对攻击方身份、何时何地采用何种手段发起攻击一无所知,处于攻防不对称的天然劣势[14]。为了改变网络空间攻守双方之间信息不对称的问题,网络欺骗技术应运而生[15]。Gartner 对欺骗技术的定义为:“使用骗局或假动作来阻挠或推翻攻击方的认知过程,扰乱攻击方的自动化工具;延迟或阻断攻击方的活动,通过使用虚假的响应、有意混淆,以假动作、误导等伪造信息达到‘欺骗’的目的。”Gartner 还指出:“到 2018 年将有 10% 的企业采用欺骗工具和策略,主动与黑客进行对抗。”

防守方一般通过诱饵、探针来诱导攻击方攻击访问蜜罐,以实现对攻击方的欺骗诱捕。诱饵是诱导攻击方访问的信息及其载体,包括代码工程文件、文档、系统旗标、密钥文件等,包含攻击方感兴趣的信息,可通过人工和自动化的方式分撒至攻击方可能访问的位置。探针是部署在业务网络内真实服务器或专用硬件设备的探针程序,监听其所处网络环境中的扫描探测行为,能够和后端蜜罐进行 1 对 1 或 1 对多的绑定,蜜罐服务通过探针映射至其所处网络中。蜜罐是采用虚拟化技术构造伪装服务,包

含Web应用、系统服务、数据库、漏洞缺陷和高级自定义蜜罐等，探针将攻击方引入蜜罐环境中后，蜜罐能够和攻击方进行交互，延缓攻击进程，诱导攻击方停留，以获取其攻击手法、真实身份等重要信息，达到欺骗诱捕的目的。

1.2 核心技术

实战攻防中欺骗诱捕技术的核心是通过虚拟化、系统进程监控模拟真实应用系统的蜜罐环境，并对蜜罐中的网络访问、指令操作等行为进行监控，对攻击行为进行告警。

1.2.1 虚拟化技术

为实现快速大量部署伪装欺骗蜜罐，需采用虚拟化技术[16]构建蜜罐组网环境，通常使用Docker容器和KVM虚拟机来实现伪装蜜罐的搭建[17-18]。

KVM技术相较于Docker技术，拥有完整的客户机操作系统，但同时需要更多的系统资源，难以实现快速的部署，二者技术对比如表2所示。

表2 KVM和Docker对比

	KVM	Docker
资源开销	较大	较小
启动时间	分钟级	秒级
镜像存储	GB级	KB-MB级
隔离级别	系统级	进程级
管理效率	低	高

选取哪种技术作为伪装蜜罐的搭建环境，应从伪装蜜罐的使用场景和功能目标来考虑[19]，兼顾高交互、高仿真、轻量化、易维护的要求[20]，蜜罐类型和虚拟化技术的对应关系如下：

(1)KVM技术：适用于主机系统蜜罐，具备完整的操作系统、中间件、数据库和其他依赖环境。

(2)Docker技术：适用于Web应用、系统服务、数据库、漏洞缺陷蜜罐，将服务封装于容器中，可快速部署和迁移等。

1.2.2 系统进程监控技术

攻击过程中通过钓鱼邮件、访问链接、安装盗版软件等操作，可以将木马、后门等恶意程序植入系统并被启动运行，作为横向攻击的跳板，因此需对蜜罐中的系统进程进行监控。

程序是指令、数据及其组织形式的描述，其本身没有任何运行的含义，是一个静态的概念；进程是计算机中的程序关于某数据集合上的一次运行活动，是程序的实体，是一个动态的概念[21]。进程的主要属性有：进程ID、进程名称、进程用户名称、进程状态、进程优先级、进程启动时间、包含的线程、使用的CPU时间、使用的内存、句柄等。进程的属性虽多，但在实际工作中发现，只要重点监控几个关键指标即可抓住进程的运行状态，进而对应用程序的健康状况做出正确的判断，及时监控到恶意进程的攻击行为[22]。

对进程级别的监控由于比较底层，本文研究采用两种手段：监控主动收集和进程埋点上报。监控主动收集，又分为两种方式，即通过系统接口获得系统上所有进程信息和通过性能计数器获得进程级别监控指标，两种方式都是非侵入式的，不会影响进程的正常运行，是首要考虑的监控方式。进程埋点上报，是一种常见的数据采集方式，在要精准获得进程级别监控数据时，代码埋点可能是最好的选择[23]。比如获得进程包含的活跃线程数以及可用性指标，都需要进程埋点上报才能获得比较精确的监控指标。当然进程埋点并不需要对每个进程都做埋点开发，可以在框架层面进行统一埋点，从而降低埋点开发及实施成本。

1.3 应用效果

1.3.1 异常流量监测与重定向

欺骗诱捕技术提供Linux、Windows等多种操作系统的探针程序，可部署在真实网络环境的服务主机或专用设备中，对网络中的扫描探测、攻击行为进行监听。当监测发现攻击方或扫描器进行端口扫描或入侵等异常访问时，探针将其请求流量重定向至与内部业务网络隔离的蜜罐服务，如：防守方搭建的由多个蜜罐组成的蜜网环境中[24]，实现网络层欺骗。

1.3.2 攻击预警与行为分析

欺骗诱捕技术通过监测节点重定向攻击流量，诱导攻击方访问伪装蜜罐，从而实现对攻击的预警和行为分析[25]。监测节点通过监听其部署环境的网络端口状态，能够实现对以下攻击事件危险行为的预警，如表3所示。

当监测到攻击行为后立即生成告警信息，结合伪装服务记录的攻击方行为日志，形成攻击方入侵时间线，完整记录其行为，支持日志下载、日志回放、PCAP流量下载和遗留文件下载。

表 3　攻击事件类型

危险行为	特征
扫描器查点	端口范围受到扫描,具备扫描特征
蠕虫病毒扩散	检测到已知漏洞扩散方法
口令爆破	尝试破解系统服务口令
系统登录	检测到伪装服务已被成功登录
Shell 执行	登录蜜罐系统后执行 Shell 指令
数据库操作	对数据库蜜罐执行操作
特定漏洞利用	检测到伪装缺陷的利用载荷

有些攻击方在业务系统或其他互联网应用中会遗留身份信息,通过记录和分析攻击方的行为特征,防守方可进一步分析其真实身份和攻击目的,准确定位攻击方真实身份。完整的入侵时间线及记录文件可作为追究其法律责任的有效证据,对攻击方实现震慑。

1.3.3　攻击方溯源

欺骗诱捕技术能获取攻击方的设备指纹、社交信息、位置信息等,以协助用户定位真实攻击方。通过 WebRTC 技术和身份溯源技术可以获取到攻击方的主机信息、浏览器信息、社交账户信息、真实 IP、代理 IP 等[26],以上信息可以帮助用户快速定位攻击方。

2　欺骗诱捕平台的搭建及测试效果

基于实战攻防对提升主动防御能力的需求,根据对攻击流程分析和气象部门业务特点,我们采用基于蜜罐的欺骗诱捕平台,构建主动防御体系,实现对异常网络流量的监测、分析和预警,并对攻击方进行诱捕、溯源。作为防守方在参与攻防演习活动时,我们采用平台进行布防,在互联网和内网分撒诱饵信息,在互联网安全区、办公内网区部署探针,构造了虚实结合的网络环境[27],欺骗和诱捕攻击方,实现和攻击方主动对抗,取得了较好的防守效果。

2.1　系统架构

欺骗诱捕平台(以下简称“平台”)提供基于蜜罐技术的伪装欺骗环境,通过分撒诱饵,诱导攻击方访问探针节点,进而将访问流量牵引至蜜罐环境中。系统监控攻击方逐步上钩的流程,将实时攻击数据同步至情报分析模块,辅助安全运营决策,同时支持实时策略配置下发,调整布防策略。平台架构如图 1 所示。

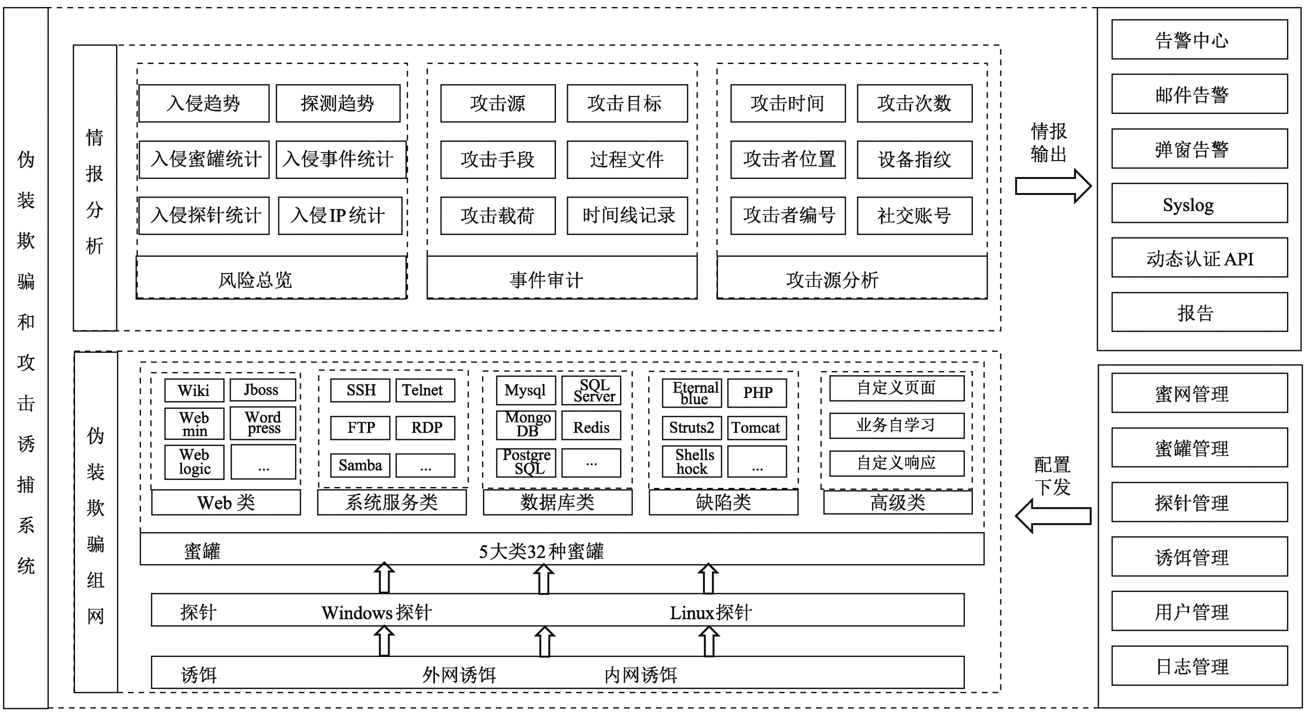

图 1　欺骗诱捕平台架构

平台由诱饵、探针和蜜罐等伪装欺骗组网模块以及情报分析模块组成。情报分析模块包含风险总览、事件审计、攻击源分析等核心功能,为用户提供威胁感知、事件处置的闭环处置流程。情报分析模块部署在安全管理区中,探针部署在内部业务网络各个区域中,探针和情报分析模块通过加密通道通信。情报分析模块能够监控探针所在网络中的各类异常行为,并通过对外映射蜜罐服务,诱导攻击方访问,从而使攻击方远离真实资产,同时对攻击方行为进行实时监控和记录,为进一步安全处置提供情报。

2.2 诱饵及探针设置

诱饵用来引导攻击方,可采用代码文件、文档和域名的方式,诱导攻击方进行访问。探针用于感知攻击方的攻击行为。

2.2.1 外网诱饵

通常利用可公开访问到的信息,如Git项目、网盘文库和域名服务系统等,进行外网诱饵的投放。特别地,可以在对社会共享的气象信息中投放探针的链接地址作为诱饵。

Git项目诱饵,利用平台生成Git项目,上传至GitHub代码托管平台。项目文件中须投放探针地址(域名或IP地址)作为蜜罐指向信息,诱饵应多方面考虑其“真实性”,加入单位信息、系统名称、项目关键信息、资产信息、项目搜索关键词等内容。

网盘文库诱饵,利用网盘文库的信息共享功能,编写单位内部信息系统测试方案、信息系统使用手册、信息系统资产列表等办公文件,投放至各类网盘文库中,便于攻击方利用信息搜集手段快速搜集。

域名诱饵,在渗透测试的信息搜集阶段,攻击方通常会使用子域名爆破、DNS查询、Googlehack等手段快速获取目标发布在互联网上的应用服务,因此可通过在主域名下创建不同的子域名并绑定探针IP地址,诱骗攻击方对蜜罐进行攻击。攻击方的域名字典中一般会包括常见子域名以及根据指定格式批量生成的子域名,因此在投放域名诱饵时,可综合生成冷门子域名以及常用子域名,以引起攻击方的关注。

2.2.2 内网诱饵

通常利用单位内部资源,如终端服务、数据库、邮件和气象观测系统[28]等,进行内网诱饵的投放。

终端服务诱饵主要是通过在提供FTP、SSH或Windows远程桌面等服务的蜜罐内部放置文档、shell历史执行命令、SSH公钥等诱饵,引导攻击方访问。数据诱饵是在数据库类蜜罐中放置虚假数据,包含其他蜜罐IP、账号口令等信息,通过虚假数据诱饵与其他蜜罐关联。邮件诱饵是在邮件蜜罐中,创建不同邮箱账号并分别放置不同种类的虚假邮件收件信息和发件信息,投放“某某系统弱口令整改通知”、“某某系统口令重置”和“知识库系统信息更新通知”等相关主题,同时可将其他蜜罐信息作为诱饵插入在邮件正文中,实现与其他蜜罐系统的关联。

2.2.3 探针部署

为能达到全网威胁感知效果,欺骗诱捕平台部署探针应覆盖重要业务系统所涉及的各个网段,重点是互联网安全区和内网的数据中心区,如气象大数据云平台[29]等。一般利用所需部署网段的空闲IP地址进行部署,伪装出带有明显漏洞的服务端口,后端与蜜罐进行关联绑定,当有攻击流量触碰到探针时,流量会被隔离并转发到蜜罐。

2.3 蜜罐配置

2.3.1 互联网安全区蜜罐配置规划

鉴于互联网安全区对外提供服务的特点[30],选取自定义Web页面、仿真页面蜜罐、邮件蜜罐、VPN蜜罐等,通过探针节点、绑定域名对外发布,诱导攻击方访问蜜罐,从而对攻击方进行攻击诱捕。B/S架构业务系统通常包含系统服务、数据库服务、Web服务等[31],因此在伪装业务系统时应综合考虑业务类型、业务组成架构,合理搭配探针所需绑定的蜜罐服务,避免选取过多无关的蜜罐。蜜罐中设置虚假数据,诱饵数据,增强伪装性和诱导性,避免使用默认配置。

2.3.2 办公内网区蜜罐配置规划

办公内网区中选取OA系统蜜罐、仿真测试蜜罐等,构建虚假的内部系统,监测办公网内异常访问行为。由于办公终端多为Windows操作系统,因此要多设置Windows服务、远程桌面协议(RDP)蜜罐,对攻击方信息收集造成混淆影响。

此外,由于办公内网区的文件交互频率较高,而工作人员安全意识水平各不相同,极易造成各类木马病毒的传播扩散,因此在办公内网区探针上通过选取绑定具有漏洞缺陷的蜜罐,也可用于协助发现感染僵尸、木马、蠕虫的终端情况。

2.4　实战效果

近两年的网络安全实战攻防演习中,我们应用伪装欺骗和攻击诱捕技术在气象业务系统外围构建了主动防御系统。以下场景描述了在攻击溯源和阻断横向移动攻击方面取得的防守成果。

场景 1:外网攻击和溯源

(1)攻击方信息收集阶段发现 DMZ 某网站 8080 端口开放一个 Web 服务(实际为防守方部署的外网诱饵);

(2)攻击方尝试通过指令或浏览器访问对该 Web 服务进行攻击;

(3)攻击流量被探针转发至 DMZ 区欺骗诱捕平台仿真页面蜜罐中,平台收到攻击告警,并对攻击方身份进行溯源分析。

(4)根据攻击方网络身份线索确定其社交媒体帐号和手机号,最终获得攻击者真实身份,完成精准画像。

场景 2:边界被突破,攻击方在 DMZ 横向攻击

(1)攻击方利用某网站漏洞突破边界防护进入 DMZ 后开展横向攻击,扫描探测发现 DMZ 区有 Windows 系统开启 RDP 服务(实际为防守方部署的内网诱饵);

(2)攻击方利用工具获取 RDP 访问权限,并进行交互操作;

(3)攻击流量被探针转发至欺骗诱捕平台的 Windows 系统蜜罐,平台收到扫描和入侵告警,对攻击方使用的 DMZ 跳板机信息进行收集,推动后续处置。

3　小结

当前各级攻防演习活动日趋常态化,伪装欺骗和攻击诱捕技术为防守方提供了一种主动对抗的手段,显著加强了防御能力。本文介绍的技术方法在国家级和气象部门内部演习活动中均获得了成功的应用,改变了攻守双方情报信息不对称的现状,为防守方建立了技术优势,在攻防演练实战中取得明显成效,保障了气象部门业务系统的安全。但是攻防对抗是持续发展和动态变化的过程,随着攻击手法的发展变化和 IT 技术的演进,伪装欺骗和攻击诱捕技术也处于不断发展之中,如:支持更多复杂协议仿真的高效费比中交互蜜罐、可与威胁检测系统智能联动的漏洞诱捕能力、持续迭代升级的溯源反制技术等[32],为完善网络安全防护体系提供重要的主动防御能力。

参考文献

[1] 宋汀.2019 年涉华 APT 态势简析[J].中国信息安全,2019,12:86-89.

[2] 国家网络空间安全战略[EB/OL].(2016-12-27)[2022-03-24].http://www.cac.gov.cn.

[3] 李欣,高见.网络攻防演练及其现实意义[J].中国信息安全.2019(1):33-35.

[4] 周云峰,叶大区.通过实战攻防演习审视政务网络安全体系建设[J].中国信息安全.2019(1):43-45.

[5] 罗玺,罗红,刘洪坤.网络攻击源隐藏技术研究[J].计算机安全,2011(11):25-28.

[6] 李杰,滕斌,曹国江.基于 CimCmdlets 的横向移动攻击检测研究与实现[J].通信技术,2019(12):3005-3009.

[7] 刘然,李小汝,陈永涛,贺俊彦,朱玲玲.气象云会商系统的设计及应用[J].气象科技,2021,49(5):723-729.

[8] 朱男男,左涛,苏杭.台风“摩羯”和“利奇马”经渤海强度变化特征分析[J].气象科技,2022,50(2):214-223.

[9] 李国翠,钤伟妙,李禧亮.“16・7”石家庄特大暴雨多源观测信息特征分析[J].气象科技,2022,50(2):234-242.

[10] 胡争光,薛峰,于连庆. 海量气象数据计算处理及可视化在决策气象服务移动平台上的应用[J].气象科技,2020,48(5).615-621,730.

[11] 秦运龙,王迎迎,张冰松,等.省级外网气象大数据服务平台研究与实现[J].气象科技,2020,48(6): 823-828,854.

[12] 刘雪花,丁丽萍,郑涛,等.面向网络取证的网络攻击追踪溯源技术分析[J].软件学报,2021(1):194-217.

[13] 陈周国,蒲石,郝尧,等.网络攻击追踪溯源层次分析[J].计算机系统应用,2014(1):1-7.

[14] 孙文君,苏旸,曹镇.非对称信息条件下 APT 攻防博弈模型[J].计算机应用,2017,37(9):2557-2562.

[15] 贾召鹏,方滨兴,刘潮歌,等.网络欺骗技术综述[J].通信学报,2017,38(12):128-143.

[16] 韩同欣,何文春,吴鹏,等.气象基础设施云平台关键设计与实现[J].气象科技,2022,50(2):290-296.

[17] 马永,王萍,管建超.基于 Docker 的应用资源池技术研究[J].电力信息与通信技术,2018,16(8):49-52.

[18] 刘文钊,黄英姿,杨冰,等.采用虚拟化技术构建新型数据中心的研究与应用[J].电力信息与通信技术,2015,13(10):7-10.

[19] 林阳阳.蜜罐技术在网络安全领域中的应用[J].数字技术与应用,2019,37(12):193-195.

[20] 赵军.高伪装高交互蜜罐技术的研究与实现[J]. 计算机工程,2010,36(15):156-158.

[21] 刁慧丹,严承.基于 Windows 内核进程监控机制的研究与实现[J].信息安全与技术,2014,5(10):42-44.

[22] 刘哲元,慕德俊.安全虚拟环境中的进程执行精确监控[J].西安电子科技大学学报(自然科学版),2012,39(6):181-186.

[23] 廖爱红,罗铭涛.埋点管理系统分析与设计[J].办公自动化,2020,25(16):33-35.
[24] 王浩淼.基于行动特征的APT攻击追踪溯源浅析[J].网络安全技术与应用,2019(8):23-25.
[25] 杨美月,钟楠宇,吴嘉熙,等.使用机器学习技术识别Web攻击方[J].电脑知识与技术,2019,15(20):237-240.
[26] 李晓云.基于浏览器脚本注入的追踪溯源技术研究[D].北京:北京邮电大学,2019.
[27] 夏刚,马钰博.混合网络蜜罐技术在互联网边界安全的研究[J].中国金融电脑,2019(9):71-76.
[28] 王小兰,张雪芬,张婷,等.气象观测设备测试与试验系统设计与实现[J].气象科技,2021,49(5):707-715.
[29] 刘媛媛,何文春,王妍,李江涛,白金婷.气象大数据云平台归档系统设计及实现[J].气象科技,2021,49(5):697-706.
[30] 刘金长,赖征田,杨成月,等.面向智能电网的信息安全防护体系建设[J].电力信息化,2010,8(9):13-16.
[31] 赵宏伟,秦昌明.基于B/S 3层体系结构的软件设计方法研究[J].实验室研究与探索,2011,30(7):64-66.
[32] 陈瑞东,张小松,牛伟纳,等.APT攻击检测与反制技术体系的研究[J].电子科技大学学报,2019(6):870-879.

Application of Deception Trapping in Defending Against Cyber Attacks in CMA

ZHOU Yan　MA Qiang
(National Meteorological Information Centre, Beijing 100081)

Abstract: With the rapid development of information technology, the cyber security situation is becoming more and more severe. The meteorological department has organized network attack and defence exercises to test and improve the capability of the service security protection system with practical standards. In the drill, the attacking team penetrates the real network and information system of important operational units. Each unit acts as the defender to carry out real-time monitoring and emergency response. Because of the information imbalance between the two sides, the defence is often in a passive situation by using traditional defence means. In order to improve the network defence capability, this paper studies the application of camouflage deception and attack trapping technology in the actual scenario of cyber security in meteorological departments. By adopting a honeypot-based deception trapping platform, an active defence system is constructed to realize the monitoring, analysis and early warning of abnormal network traffic, and trap and trace the source of attackers. Through actual combat tests, the application of deception trapping technology has effectively improved the cyber security defence capability and ensured meteorological operational systems stable and reliable.

Keywords: cyber security; cheating trap; offensive and defensive confrontation; traffic redirection; behaviour analysis