简译版

有效诱捕的七个技巧

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	7 Tips for Effective Deception		
原文作者	杰·维贾扬（Jai Vijayan）	**原文发布日期**	2020年6月25日
作者简介	杰·维贾扬是一位经验丰富的技术记者，在IT贸易新闻领域拥有20多年的经验。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/vulnerabilities---threats/vulnerability-management/7-tips-for-effective-deception/d/d-id/1338175		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

有效诱捕的七个技巧

杰·维贾扬

2020 年 6 月 25 日

恰当的诱饵能够挫败攻击者，有助于企业更快地检测到威胁。

攻击者攻破企业网络（有的网络防御措施良好）的能力日益增强，导致近年来企业对诱捕技术和策略的兴趣日益浓厚。

诱捕工具主要使用误导、虚假响应等技巧诱导攻击者远离目标，进入蜜罐等诱饵系统，这些系统旨在诱捕攻击者或分散其注意力。诱捕工具（其中许多工具利用了人工智能[AI]和机器学习[ML]技术）可以帮助企业及早发现入侵活动，为其提供观察攻击者工具和策略的机会。

在最近的一份报告中，分析公司 Mordor Intelligence 预测，企业对诱捕工具的需求将从 2019 年的不到 12 亿美元增长到 2025 年的约 25 亿美元。该公司指出，大部分需求将来自政府部门、全球金融机构以及其他频繁遭受网络攻击的目标。

Attivo Networks 首席技术官托尼·科尔（Tony Cole）说，诱捕是一个有趣且非常古老的概念，在过去的几年中非常热门。

他说："企业几乎可以在任何可能发生攻击的地方部署诱捕手段。"他补充说，在端点保护、端点检测和响应工具保护不到位的情况下，诱捕将特别有用。"例如，当攻击者攻击一个端点，利用它来查询 Active Directory 时，企业可以向攻击者提供虚假信息，从而导致攻击者远离真实的攻击目标，而不会影响其生产环境。"

Acalvio 首席营销官里克·莫伊（Rick Moy）介绍了三个主要诱捕用例：（1）在关键任务环境中增加保护层；（2）增强在已知安全漏洞方面的检测能力；（3）诱骗隐藏在大量安全信息和事件管理（SIEM）告警中的攻击者。

莫伊说："在各网段中部署的诱饵，相当于沿着厨房踢脚线放置的捕鼠器中的奶酪或花生酱。"

根据莫伊等人的说法，以下是使用诱捕手段快速检测威胁的七个最佳实践。

使用真实计算机作为诱饵

KnowBe4 数据驱动防御推广师罗杰·格里姆斯（Roger Grimes）说，最接近真实生产资产的诱饵是最好的诱饵。如果诱饵系统与其他系统有明显的不同，攻击者就会有所发现，因此关键在于使诱饵系统看起来像真实的生产系统。格里姆斯说："攻击者无法分辨真实生产资产与仅存在于蜜罐中的生产资产。"

企业可以将老旧并打算退役的系统作为诱饵，也可以将类似企业环境中其他服务器或设备的新服务器作为诱饵。格里姆斯指出，诱饵系统应使用与真实生产系统相同的名称，放置在相同的位置，并部署相同的服务和防御措施。

Acalvio 公司的莫伊说，关键是要"以假乱真"。企业应避免使用明显的迹象，例如通用 MAC 地址、常见的操作系统补丁级别以及与该网络上的通用约定不符的系统名称。

确保诱饵看起来重要和有趣

攻击者讨厌诱捕，因为诱捕会导致他们掉入陷阱。Crypsis Group 首席顾问杰里米·布朗（Jeremy Brown）说，高明的诱捕手段可以干扰攻击者，使其停止入侵活动数小时、数天甚至数周。

他说："一种诱捕方法是建立虚拟服务器或物理服务器，这些服务器看起来像是存储着重要信息。"例如，运行真实操作系统（例如 Windows Server 2016）的诱饵域控制器对攻击者就非常有吸引力。这是因为域控制器包含 Active Directory，而 Active Directory 则包含企业环境中所有用户的权限和访问控制列表。

吸引攻击者的另一种方法是：创建不活跃使用的真实管理员账户。攻击者喜欢寻找赋予他们更高权限的账户，例如系统管理员、本地管理员或域管理员账户。布朗说："如果发现搜索此类账户的活动，就说明攻击者进入了网络。"

模拟非传统终端设备

Fidelis 公司产品副总裁蒂姆·罗迪（Tim Roddy）说，在企业网络上部署诱饵时，不要忘记模拟非传统端点。越来越多的攻击者开始寻找和利用物联网（IoT）设备和其他联网非 PC 设备中的漏洞。罗迪说，企业应确保在其网络上部署诱饵，如监控器、打印机、复印机、运动监测器、智能锁以及其他可能吸引攻击者注意的联网设备。

也就是说，诱饵应与攻击者期望找到的设备一起融合到企业网络中，包括物联网设备。

像攻击者一样思考

在部署诱饵系统和诱饵时，企业应考虑：最具杀伤力的攻击者会对企业网络造成什么样的影响。Acalvio 公司的莫伊说："企业应根据这种思想来制定优先检测目标清单，以弥补防御系统中的漏洞。"

此外，企业还要考虑攻击者为实现目标可能采取的措施，并据此布置"面包屑"，这些"面包屑"指向与攻击者所求目标有关的诱饵。例如，如果攻击者的目标是凭证，企业应部署伪造凭证和其他基于 Active Directory 的诱捕手段，莫伊说。

使用正确的"面包屑"诱骗攻击者

入侵员工 PC 的攻击者通常会搜索注册表和浏览器历史记录，以查看该用户在何处查找内部服务器和打印机等设备。Fidelis 公司的罗迪说："'面包屑'是指模拟这些设备的诱饵的地址。"

一个好办法是：将诱饵的地址分配给最终用户设备。罗迪说，如果设备受到攻击，说明攻击者跟随'面包屑'进入了诱饵，进而为管理员发出告警。

主要将诱捕用于预警

不要仅使用蜜罐等诱捕手段来跟踪或确定攻击者的行为。KnowBe4 公司的格里姆斯说，这样会得不偿失。相反，最好将诱捕手段作为预警系统来检测入侵，将跟踪和监控工作留给取证工具。

格里姆斯说："企业想要持续监控，需花时间排除网络上每项资产的正常生产连接，例如与打补丁和杀毒软件更新有关的连接。"攻击者不知道环境中哪些资产是伪造的，哪些资产是真实的。如果伪造的资产看起来像是真实生产资产，他们就会连接到这些资产。

"如果蜜罐被连接，就很可能是出现了恶意活动。"格莱姆斯说。"不要让告警只停留在 SIEM 事件记录中，而耽误了调查。"

保持诱捕的新鲜感

Acalvio 公司的莫伊说："任何策略都要避免陈旧"。要想更好地诱捕攻击者，企业应不

断更新其诱捕手段，以跟上用户活动、应用足迹乃至网络暴露情况的变化。他说：“例如，新漏洞可能无法修复，但可以通过诱捕手段来快速加以保护。”

使用诱捕手段可以增强在已知安全漏洞方面的检测能力。这些漏洞可能包括：难以保护或打补丁的远程员工笔记本、VPN 网关网络、合作伙伴或承包商网络以及凭证等。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com