简译版

欺骗：一种令人信服的网络防御新方法

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	Deception: A Convincing New Approach to Cyber Defense		
原文作者	Ofer Israeli	**原文发布日期**	2017 年 9 月 12 日
作者简介	Ofer Israeli 是以色列网络安全公司 Illusive Networks 的创始人和首席执行官。https://www.darkreading.com/author-bio.asp?author_id=2528		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/threat-intelligence/deception-a-convincing-new-approach-to-cyber-defense/a/d-id/1329839?		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
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。		

欺骗：一种令人信服的网络防御新方法

Ofer Israel

2017 年 9 月 12 日

美国国家安全机构的防御者如何在捕获标识演习中使用虚假数据来挫败攻击者并遏制伤害。

我们生活在攻击向量不断增加的世界中。黑客们使用越来越粗暴的方法攻破边界防御，包括窃取的凭证和后门、网络钓鱼、间谍软件和恶意软件，暴力破解等等。一旦攻击者成功地攻破了网络，他们通常会有足够的时间造成重大损害。根据威瑞森《2016 年数据泄露调查报告》，只有 25%的感染持续“几天或更少的时间”，火眼公司 2017 年 M-Trends 报告显示，尽管检测方法持续改进，发现网络攻击的平均时间仍然长达 99 天，其中，47%的感染是由外部来源（如联邦调查局）通知受害者的。

没有一个解决方案能够阻止所有形式的攻击，同时遏制攻击导致的损害。就像一个由陆军、海军和空军组成的军队一样，每个军种都有多种武器和人员，网络安全防御系统必须能够预见所有可能的威胁向量，并开发多种机制来对抗它们。

人们对欺骗方法（最新的网络安全方法之一）的认识正在增加。Gartner 称之为“威胁欺骗”，并预测 10%的企业将在 2018 年之前采用某种形式的网络欺骗手段。欺骗依赖于攻击者的一个漏洞：攻击者认为他们在网络上找到的信息是真实的，他们收集的数据是可靠的。欺骗策略利用了这种漏洞，在企业端点、网络、数据和应用程序中放置看似真实的虚假信息。当边界防御失败后，攻击者就无法区分真实数据和欺骗数据了。

高级攻击者如何接近网络呢？首先，与电影中的形象不同，黑客使用各种工具和技术，缓慢而有条理地收集数据、分析数据，并在整个网络中横向运动。最初，当访问网络时，他们会有一点困惑。他们不知道到了哪里，也不知道目标在哪里。通过反复尝试，他们构建了网络环境的映射：网络本身以及它的使用方式。例如，他们可能会从一个员工的电脑中发现 SharePoint 服务器的线索，由此找到有关的文件和名称，这有助于他们确定下一步的行动。攻击者越高级，其横向运动方法就越复杂；横向运动越多，映射就越详细。这种迭代过程使他们最终能够找到并感染目标。

当攻击者在网络中运动时，捕获他们的一种常见策略是蜜罐。蜜罐看起来像 PC 或服务器，其理念是，当攻击者访问蜜罐时，蜜罐会发出告警，提醒 IT 人员发生了攻击。蜜罐的问题是它们的部署和管理很费时，所以使用相对较少，这意味着当攻击者访问蜜罐时可能已经发生了重大感染事件。更糟糕的是，经验丰富的黑客很容易识别蜜罐。

欺骗和“捕获标识”

威胁欺骗采取不同的方法。红军演习的过程能够很好地阐释欺骗技术，以及欺骗技术的有效性。美国国防部门设立了一项“捕获标识”演习，以测试欺骗战略的有效性。一个团队作为攻击者，他们执行多次攻击以捕获和检索被防御团队保护的目标。攻击团队不知道对方部署了欺骗战略。然后，防御团队在端点、服务器和攻击面上引入了各种虚假数据。欺骗类型包括“分享欺骗”（诱骗攻击者访问假的共享文件夹和文件），“Windows 凭证欺骗”（使用不存在的用户凭证诱骗攻击者）和“文件欺骗”（诱骗攻击者访问和使用存储在假文件中的凭证）。这些欺骗手段是精心制定的，以确保在攻击者看来是真实的。

为了部署欺骗策略，防御团队使用了两个组件：一个用来传播欺骗信息的服务器和一个陷阱服务器。作为低成本的无代理解决方案，欺骗策略对网络服务和性能几乎没有影响，并且具有高度可扩展性。这些欺骗策略部署在整个企业的现有工作站、笔记本电脑和服务器上，不需要特殊的硬件。此外，网络的合法用户从不会访问这些欺骗信息，所以他们的工作不受影响。这也大大减少了误报数量。

当攻击团队发动攻击时，他们会立即发现欺骗信息，这些信息正是他们在网络中横向运动所需要的。访问这些欺骗信息会触发陷阱服务器，它会提醒防御团队发生了攻击。陷阱服务器就像一个真正的服务器；当攻击者遇到它时，就会像平常一样筛选它包含的信息，但是在这种情况下，数据是假的。陷阱服务器还对攻击源进行实时取证，帮助防御团队确定攻击者的目标，并提供可操作的证据和制品来帮助他们遏制攻击。在真正的攻击中，取证分析对执法机构来说是非常有价值的。

同样，一家面临越来越多的金融威胁的大型国际银行也部署了欺骗策略来补充现有的网络安全工具，并增加一种新的、更直接的威胁检测能力。该银行采用与美国国防部门类似的方法，为共享文件夹、服务器、Windows 凭证、SWIFT 和其它网络系统部署了一系列欺骗方案。随着欺骗解决方案到位，银行实现了接近即时检测的目标，误报率很低。当告警被触发时，安全团队能够观察攻击者在网络中的横向运动，收集取证数据，并监控攻击行动。这

使得防御团队更具战略性，在造成损害之前终止攻击。

网络犯罪分子将会越来越聪明，越来越大胆。为了保护您的网络，您必须不断加强防御措施。欺骗方法是一种强大的、先发制人的、互补的防御解决方案。如果您负责保护网络和数据资产，您应该考虑欺骗策略。