



## 攻击信标（IOA）与攻陷信标（IOC）





# 攻击信标 ( IOA ) 与攻陷信标 ( IOC )

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	Indicators of Attack versus Indicators of Compromise		
原文作者	CrowdStrike	原文发布日期	
作者简介			
原文发布单位	CrowdStrike		
原文出处			
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 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"><li>• 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。</li><li>• 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。</li><li>• 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。</li><li>• 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。</li></ul>		



攻击信标 ( Indicators of  
Attack , IOA )

攻陷信标 ( Indicators of  
Compromise , IOC )

## 两者有何不同？

对于有责任保护宝贵数据的企业而言，网络威胁从未如此严重。最近，网络攻击事件不断登上新闻头条。这说明，没有哪家公司或机构能够完全免受高级持续性攻击者的针对性攻击。

这些攻击针对全球装备精良的大型企业，并不断取得成功。这导致许多安全高管质疑，传统分层防御解决方案能否有效防御针对性攻击。同时，许多企业开始在遭受网络攻击之前审查和修订其最佳安全实践。

译者注：IOA 是攻击尚未得手，对被攻击系统表现的各种即时特征；属于进行时。IOC 是攻击得手后，被攻陷系统的各种现实状态；属于过去式。



## IOC 和 IOA 的根本差异

如下图所示，IOC 是一种被动的方法。恶意软件、特征、漏洞利用代码、漏洞和 IP 地址等信标的存在，是发生攻击的典型证据。与此相反，IOA 是一种主动的方法——防御者主动寻找可能发生攻击的预警信号，例如代码执行、持久驻留、隐蔽、C&C 和网络内的横向移动等。IOC 和 IOA 的区别类似于：犯罪发生后到达犯罪现场，根据遗留的证据重现犯罪过程 vs 警惕更细微的信标，阻止即将发生或正在进行的攻击。





## 现实世界的类比

我们采用现实世界的事件进行类比。有一家银行遭到抢劫，警方赶到，开始收集证据。例如，监控探头可能会记录下，劫匪开着一辆紫色货车，戴着巴尔的摩乌鸦队球迷帽，使用液氮打开保险库。这些证据都表明，银行确实遭到抢劫了。钱款损失已经造成；但是，通过追踪证据，警方可能会抓到劫匪——除非劫匪改变其作案方式（MO）。但是，如果同一个劫匪下次开红色轿车，戴牛仔帽，利用撬棍进入保险库，又会怎样呢？他会再一次成功进行抢劫，因为监控团队依赖的是过时的 IOC。

反之，如果调查人员使用基于 IOA 的方法，结果可能会大不相同。例如，聪明的劫匪首先要对银行“踩点”，进行侦察，了解其防御漏洞。一旦劫匪确定了最佳的抢劫时间和战术，就会进入银行。他会先破坏掉安全系统，然后走向保险库，试图破解保险库的密码。如果银行的安全团队能够发现抢劫之前的“踩点”行为——换句话说，如果他们能够识别 IOA，就有可能在劫匪抢劫之前将抓住。



在信息泄露的情况下，IOC 可能包括各种电子证据，如 MD5 哈希、C2 域、硬编码 IP 地址、注册表项、文件名等。然而，这些 IOC 会不断变化，因此安全团队无法采取主动的方法来保护企业。IOC 是一种反应式的追踪方法，当安全团队找到一个 IOC 时，企业很有可能已经被攻陷了。

相比之下，IOA 代表了攻击者为取得成功所必须采取的一系列行动。我们以意志坚定的攻击者最常用、最成功的攻击方法——鱼式网络钓鱼攻击——为例进行分析，来说明这一点。

成功的网络钓鱼邮件必须说服目标用户点击链接或打开会感染计算机的文档。一旦计算机受到感染，攻击者就会悄悄执行隐藏在内存或磁盘上的另一个进程，即使系统重启该进程也能驻留。之后，该进程与 C&C 站点取得联系，等待攻击者发送下一步指令。



IOA 关注的是这些步骤的执行，而这些步骤揭示了攻击者的意图及其试图达到的结果。IOA 并不关注攻击者用来实现目标的特定工具，能够追踪其不断变化的战术。

通过监控这些步骤、收集信标并对其进行分析，我们可以确定攻击者如何成功获得网络的访问权限，并推断其意图。我们不需要事先了解特定工具或恶意软件，就可以在攻击发生时加以阻止。事实上，IOA 可以检测不使用恶意软件的攻击。

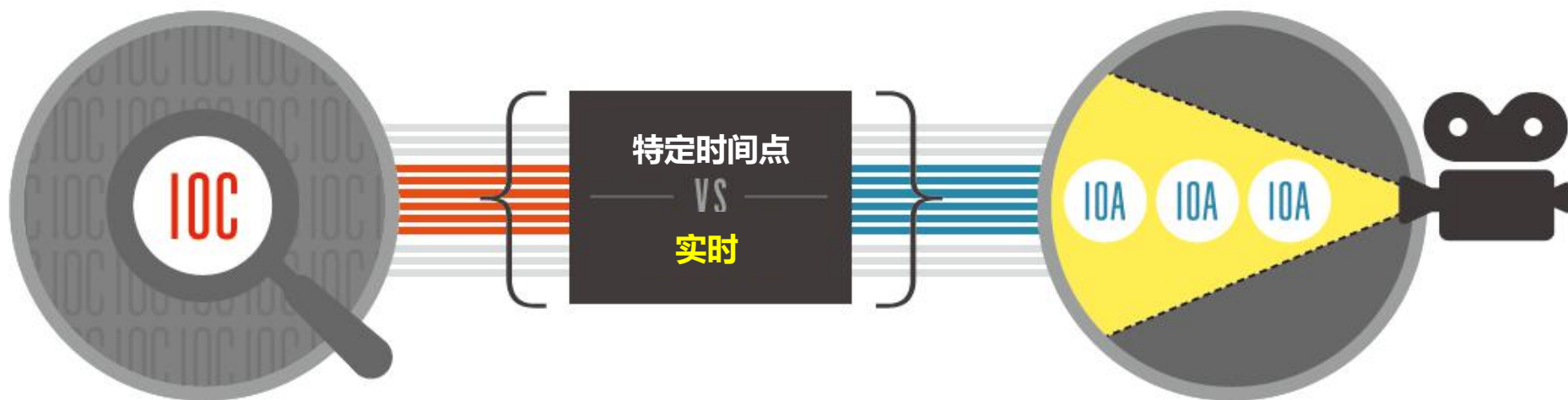
## 攻击信标



## IOA 提供实时记录和可见性

通过基于 IOA 的方法，安全团队能够实时、准确地收集和分析网络上正在发生的行为。观察这些行为就相当于，盯着企业环境中的监控探头并随时访问数据记录器。

通过记录每一个行为发生的过程，IOA 能够准确地展示攻击者是如何潜入企业环境、访问文件、转储密码、在企业网络中横向移动，以及最终窃取企业数据的。





## 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>