# 安天周观察

主办：安天　2017 年 8 月 7 日（总第 98 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流


## 安天发现新型 DDoS 攻击木马“魔鼬”

7 月 30 日，安天安全研究与应急处理中心 (Antiy CERT) 的工程师发现一种具备拒绝服务 (DDoS) 攻击能力的新型木马。经初步分析，安天 CERT 工程师认为该木马属于一个新家族，并将其命名为“魔鼬”。通过关联查询安天对于 DDoS 攻击的历史监测数据，发现本次事件中受攻击的域名同时也在遭受 Trojan/Linux.BillGates、Trojan/Linux.Mayday 等家族的 DDoS 攻击。

从目前掌握的资料来看，本次 DDoS 事件的攻击强度足以瘫痪一般的网站，但是部分受攻击网站采用了 CDN 服务，因此没有受到严重影响。该木马家族的出现时间仅有短短的 1 个月，却发现较多起由该家族发起的 DDoS 攻击事件，说明该木马传播速度较快，需要引起重视。

对于本次事件，安天建议用户尽快排查自身网络内是否有 C2 地址及被攻击目标地址的访问，并对可疑终端进行检测与排查，一旦发现有终端主机对上述地址有大量请求、连接极有可能已感染该木马程序。请您联系安天寻求专业帮助：400-840-9234。

安天再次提醒用户，安装能力型安全厂商提供的终端安全产品，推动积极防御、威胁情报与架构安全和被动防御的有效融合，建立攻击者难以预测的安全能力，达成有效防护和高度自动化和可操作化的安全业务价值。

## 安天收到深圳市公安局网警支队八大队感谢信

近日，深圳市公安局网络警察支队八大队向安天发来感谢信，感谢安天在涉深圳的一起 DDoS 攻击案侦破工作中做出的贡献。7 月，安天配合八大队成功锁定了涉深圳的一起 DDoS 攻击案的攻击源。安天在本次案件中，服从警务人员的安排，努力做好技术支撑工作，提供的攻击源数据大大节省了案件的侦破时间，安天技术人员的过硬素质得到了该案参与人员的一致好评。

随着网络攻击案件的增多，网络安全防护战需要警民协作，线上线下、群防群治，公众安全才会得到有力保障。习总书记在 4·19 讲话中强调“只有积极承担社会责任的企业才是最有竞争力和生命力的企业”，安天在发展过程中始终践行企业的社会责任，积极运用 17 年积淀的威胁检测防御技术和监控预警能力服务社会，安天作为网络安全应急服务支撑单位之一，多次在重大网络事故和网络安全事件的响应中发挥关键作用，今后，安天会一如既往在维护国家网络安全的工作中，贡献自己的一份力量。

## 肖新光：态势感知的支撑和价值落地

### ——2017 网络安全生态峰会演讲全文

（第 2-4 版）

## ■ 银行木马 Trickbot 变种新添蠕虫病毒攻击模块

近日，安全专家发现黑客通过银行木马 Trickbot 新变种的蠕虫病毒攻击模块肆意传播国际金融垃圾邮件，旨在瞄准全球银行系统展开新一轮攻击活动。 Trickbot 新变种允许黑客发起定向攻击，诱导用户访问恶意网站输入个人凭据。据悉，攻击者大规模增加垃圾邮件每日数量、肆意传播 Trickbot，以致影响全球用户及各个地区金融指标。目前，黑客正测试 Trickbot 新模块，即蠕虫病毒横向移动功能，允许感染同一局域网 (LAN) 上的其他计算机系统并将其作为僵尸网络分发传播恶意软件。尽管蠕虫模块的当前形式过于简单，但很显然该组织是通过复制勒索病毒 WannaCry 与 NotPetya 的攻击方式后深入研究而成。（来源：http://hackernews.cc/archives/12882）

## 安天开展庆祝建军 90 周年观影活动

8 月 1 日，为庆祝中国人民解放军建军 90 周年，增强爱国主义情怀，安天哈尔滨总部组织大家一起观看了军事电影《战狼Ⅱ》。在紧张的工作之余开展观影活动，不仅为了丰富公司员工业余生活，建设企业文化，增强集体凝聚力，英雄主义动作片《战狼Ⅱ》燃烧的爱国主义情怀让同事们热血沸腾，更加坚定了安天人在网络空间为国铸盾的雄心壮志。

在维护国家网络安全的道路上，安天战士们始终站在直面对手的第一线，以对手能力检验和提升产品与服务能力。政治立场坚定可靠，技术能力自主先进。在方程式、白象等多起 APT 攻击事件的率先发现、深度分析与追踪溯源中，在破壳、魔窟等重大安全事件的应急响应中发挥了关键作用。遵道而行，但到半途须努力；会心不远，要登绝顶莫辞劳。

今后的安天人将继续践行军民融合战略，以更大的决心、更久的恒心、更准的重心为国家安全保卫工作奉献热血和力量。

# 态势感知的支撑和价值落地

本文依据安天首席架构师肖新光在 2017 网络安全生态峰会演讲整理而成

## 一、现状反思与回归本源

当前正在实施的较大比例的态势感知工程项目是基于大规模扫描探测或开源威胁情报向可视化效果的粗浅叠加，即“地图炮”，这就是态势感知当前的普遍实践。在这种庸俗化的倾向下，态势感知没有走向“鹰的眼睛、狼的耳朵（复合感知）、熊的力量（支撑体系）、豹的速度（响应）、人的大脑（决策）”，而是变成了一只“孔雀”，一种被美丽尾羽所负累的飞鸟。原本它应该是一个有效地进行观察、思考、决策的体系，但是现在其整体价值都被这种表现力所干扰。

在网络空间陷于“乱花渐欲迷人眼”之时，我们应回到传统空间去寻找一些启示和答案。网络空间并非一个完全独立于传统空间的特异性场景。比如，在传统政经领域中，对于威胁的经典认知是“威胁是能力和意图的乘积”，而在网络空间的 APT（高级持续性威胁）中：A（高级性）就是其能力，P（持续性）就是其意图，T 就是威胁，“A、P”、“T”三者之间的关系是，“T”是“A”和“P”的乘积，这是符合传统的对于威胁的认知规律的。

网络空间的威胁之所以被逐渐重视，不在于其特殊性，而在于其达成了传统空间攻击作业的等效性，并且逐步具有更高的效费比。这一点我们在之前的报告中通过对比“凋零利刃计划”、“巴比伦”行动（美国、以色列对伊拉克核反应堆的空中打击）与“震网”事件已经进行了阐述；其次，如果进一步对比“震网”事件、“乌克兰停电事件”和伪装成“必加 (Petya)”的攻击事件，可以发现网络攻击关键信息基础设施的成本正在不断降低。

在这样的认知下，网络空间领域与传统空间的特殊性、差异性，是建立在共性基础上的。

因此，我们在看待态势感知时，要回归其本源的要求。习总书记在 4·19 网信工作座谈会上要求我们实现“全天候、全方位感知网络安全态势”，结合态势感知的经典定义“在一定时间和空间内观察环境中的元素，理解这些元素的意义，并预测这些元素在近期未来的状态”，那么态势感知的要求和定义之间的映射关系是，“全天候”是一个“时间”和“条件”的概念；“全方位”是一个“空间”的概念；“感”对应“观察”；“知”对应“理解”；“网络安全”意味着对应的认知域；“态”对应“元素的意义”；“势”对应“近期未来的状态”。这是对整个态势感知的一个有效理解。而观察、理解和预测，构成了态势感知工作的三个核心环节。

想要达成一个有效的态势感知，需要像 OODA 模型、学习战机飞行员“狗斗”一样，最后形成一系列可拆解的规定动作。这种规定动作就可以转化为人借助相应的工具所能达成的手工流程，再随着整个手工流程的实践逐渐转化为一个有效的、可以由专家经验和知识学习共同推动的过程。

所以，从工程意义上来看，态势感知注定是一套业务系统，而不是“展示系统”。

## 二、改善我们的采集和对象处理

### 2.1 SOC/SIEM 与态势感知系统的差异

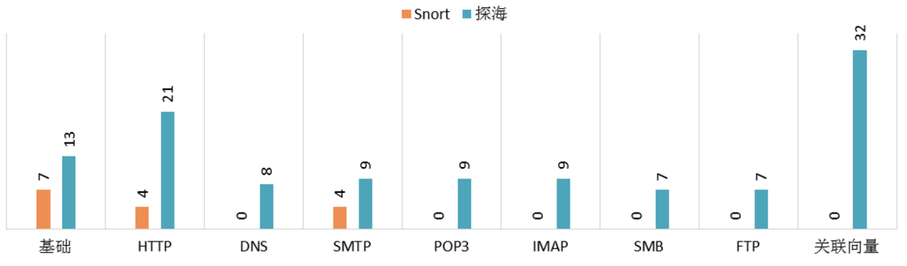
粗糙的态势感知把大规模的扫描器或开源的威胁情报叠加到可视化手段上；而业务化的部分态势感知实践，则是在传统 SOC/SIEM 的基础上做一些可视化展示能力的加强。这就带来一个很有趣的问题，从一个平台系统的角度来看，态势感知是 SIEM/SOC 的整容版吗？ SOC 源自，有大量离散的安全环节没有形成整体能力，为达成对这些安全环节的有效组织，使之成为一个相对协调的整体；SIEM 源自，由于无任何一种单一环节能采集所有信息，所以将设备、应用系统和产品的日志，以及端点侧、流量侧不同的安全产品的日志汇聚起来，基于整个安全事件与事故的数据提交形成分析能力。

SOC 和 SIEM 都有其历史价值，但 SIEM/SOC 所面临的一个情况是，它们都晚于成熟的安全产品品类产生，这就带来一个问题，这些传统产品自身的能力和采集的覆盖面积，是否能支持当前全面性的威胁对抗场景下的要求？而态势感知则是要求我们传统的有探针价值的安全产品，逐渐转化为有效的感知探针。

### 2.2 流量侧感知

以经典的开源 IDS Snort 为例，其是由被规则匹配到的事件的五元组和相应的规则名称构成相应的基础日志，其局部的扩展能力十分薄弱。这也意味着所有不能够被规则匹配的流量不会被记录，这就使得传统的 IDS 先天不会是一个完整的流量分析和记录的工具，而流量分析和记录工具往往又没有相应的威胁识别和检测能力，因此，两者都很难完整地服务于态势感知体系。

规则匹配记录异常、五元组解析对于流量侧的态势感知是不够的，需要在不同的协议分支上展开更多的采集点和基础数据，使其无论是否匹配到威胁，都会进行符合工作配置要求的持续性数据积累。基于我们根据全数据解析设计的新版探海威胁检测系统，我们对传统 IDS 的采集能力和探海的全要素采集能力进行对比，发现两者之间在采集要素方面具有较大的数量差异。




传统 IDS 的采集能力与探海的全要素采集能力对比

因此，只有形成非常细粒度的流量侧的采集能力，同时在实际场景中，根据安全需求和资源进行按需采集，并且根据专家经验渐进达到一种自适应采集的程度，才有可能在当前安全威胁日趋高级和隐蔽的情况下，在第一攻击波往往会注定性地穿透防线的情况下，达成即使威胁未被检出，但同样会形成雁过留痕的可追溯数据的能力，从而改变威胁对抗的时空。

### 2.3 文件对象处理

如果我们对流量侧和端点侧的数据进行相应的细腻解析，捕获到大量的未知文件应如何处理？作为国内最早探索沙箱技术并将其广泛应用到产品和工程实践中的团队，我们同样需要指出一种值得忧虑的倾向——正在把沙箱转化为一种合规性的环节，把沙箱视为一种鉴定器，把相应的对象丢入沙箱等候结果视为样本型对象处理的全部，却忘记了沙箱的更有效价值不是威胁鉴定，而是漏洞触发、行为揭示和威胁情报生产。沙箱是基于内部环境条件对样本进行执行分析，因此，沙箱带来的一定是样本要素的一个结果子集，不可能带来样本更全面的威胁覆盖。

实际上，大量样本在沙箱中很难形成分析结果。例如，WannaCry（魔窟）的灭活域名机制，因很多沙箱有模拟对所有域名请求进行应答的机制，这将导致其第一时间被穿透；类似“震网”的 USB 摆渡行为，是基于复杂的逻辑定义的，类似于“方程式”的主机作业模块积木，每个积木块都难以单独执行运行，也难以触发对恶意行为的加权判断。因此，简单地把沙箱当作是“放之四海而皆准”的、有效的分析环节是完全不够的，仅仅依靠动态所形成的向量拆解也是不够的。更何况，当前大量的沙箱并没有作为一种向量拆解器被使用，而是作为一种简单的动态判定器被使用。

### 2.4 载荷检测引擎：从检测器到检测分析器

除了动态分析，一个有效的对象处理还需要进行深度的静态格式解析，这就必须改造传统的反病毒引擎。对于可检出的对象，传统检测引擎仅仅能够赋予一个相应的名称，其提供了简单的分类、环境、家族和变种等信息，但是不能提供更多的信息。安天倡导下一代威胁检测引擎的意义是，其不仅仅是一个静态的鉴定器，更是具备全对象识别和解析能力的鉴定分析器。下一代威胁检测引擎可以针对任意对象输出包括检测结果和向量拆解结果的结构体，不仅具有检测功能，还能进行大量的向量提取，而利用这些提取出的向量，并经过相应的计算和标签化，就可以绘制出样本的行为，整个过程是不依赖于动态分析的。

对于传统引擎和下一代引擎均无法检出的对象，传统引擎只给出了“这个文件是 OK 的”的结果，但是下一代威胁检测引擎依然可以在无检出的情况下输出整个向量解析结果，基于这些解析结果，上层就可以通过决策来得出其具有反调试行为、键盘记录行为和获取系统信息行为等判断，从而实现向向量提取、知识标签的转化。

从传统的威胁检测引擎和对象的鉴定器来看，其存在着一种有条件的分析，即是否能够告警决定了整个威胁的价值。而对于下一代威胁检测引擎而言，不存在单纯的有毒对象和无毒对象的概念，只存在分析对象的概念，将实现对一切对象的识别和拆解，并基于拆解结果构成一个分析大数据的空间。

## 三、有效防护和价值落地

### 3.1 预见力未必能有效转化

态势感知系统首先一定是依赖于专家经验的，安天曾做出了很多获得业内好评的预测。2015 年 5 月 27 日[1]以及 2016 年 11 月 4 日[2]，我们先后在两篇报告中明确指出了网络军火失控和外溢所带来的安全问题；在 2016 年的威胁年报[3]和其他文献中，我们对“勒索病毒采用更多方式进行投放”以及“蠕虫回潮”也做出了相应的预见。但是这些预见除了带动我们自身的产品和能力升级之外，是否带动了有效的社会能力提升？我们在反思，一个安全企业向公众、主管部门释放安全信息本身也存在着最佳成本时点问题。尽管我们在 2017 年 3 月对微软针对相关 SMB 服务的补丁提出关注，对 4 月 14 日的网络军火泄漏的大规模利用也提供了预警，但是从 4 月 14 日到 5 月 12 日之间，在发现了使用“永恒之蓝”漏洞的地下黑产程序后，我们却未明确强化这一漏洞可能会被大规模使用的观点。如果相关的安全资源在这一时间点有效地、密集地投放，WannaCry 式的威胁预警就将不再是一种预言家式的过前判断，而会有效地转化为行动能力。

### 3.2 从 WannaCry 巨大响应成本看有效防护价值

我们认为 WannaCry 事件的“应急处理”总体上是成功的，但从社会机体响应情况而言，我国当前所面临的核心问题不是应急问题，而是一个无效防护的问题。

勒索软件不应该是一种依靠应急响应去做普遍性应对的威胁形式。通过针对乌克兰的模仿成“必加”的攻击可发现，这种攻击是以破坏数据为目的的，应如何进行相应的有效响应？只有通过有效防护去收窄最终的响应面，整个的社会应急成本才是收敛的。如果我们不能够普遍性地建立全社会的基础的有效防护能力，完全把相关责任抛给应急，就必然会呈现出需要处置的威胁不收敛的情况。

（下转第四版）

1 安天：《一例针对中国政府机构的准 APT 攻击中所使用的样本分析》：http://www.antiy.com/response/APT-TOCS.html
2 安天：《从方程式到“方程组”——EQUATION 攻击组织高级恶意代码的全平台能力解析》：http://www.antiy.com/response/EQUATIONS/EQUATIONS.html
3 安天：http://www.antiy.com/response/2016_Antiy_Annual_Security_Report.html

（上接第三版）

就具体的态势感知系统而言，假如在一个态势感知系统所防御的范围内，没有基础的有效的防御能力，就势必要把大量的低级化的安全事件推送到态势感知系统中，并进行相应的决策和处理，这就使得需要态势感知系统做出判断和人力研判的事件全面增加，所驱动的响应面呈现出扩散形势，导致整个态势感知变成了一个无法用来指导最终价值落地的环节，因为整个事件是不收敛的。

当然，我们并不能指望着防御能处理所有的问题，如果单点防御能够处理所有问题，那么态势感知将是无价值的，但是如果没有基础的有效的防御能力，态势感知将是无意义的。

## 四、态势感知的视角与支撑

### 4.1 视角：从以事件为中心到以资产为中心

态势感知的一个合理视角应该是什么？当我们把大规模轻载扫描的漏洞探测结果叠加到地图上，并认定这是一种态势感知时，这实际上是一种节点脆弱性视角；当我们把流量侧数据简单地叠加到可视化上时，这实际上是一种检测事件维度的视角。如果从一个偏哲学意义的角度去认识态势感知，实际上，网络威胁态势感知是一个对网络空间中的主体、客体和关系进行认识和表达的过程，主体、客体和关系是认知论中的核心要素。无论是攻击组织、用户，还是安全厂商、机构或者其中的个体，都是主体；无论是攻击者所使用的计算机网络设备和工具，还是防御方所拥有的安全资产，都是客体。就客体而言，既包括有型的服务器、设备，也包括无形的数据资产；主体和主体之间存在着相应的关系，一个主体如果想要对另一个主体进行攻击，就是相应的意图，而攻击从攻击方的客体设施到达防御方的客体资产，就构成了关系。因此，安全事件是一个关系表达。

### 4.2 从威胁检测到威胁认知的提升

从这个角度来看，态势感知在很大程度上并不是一个威胁检测环节，它带来了威胁认知模式上的演进。从安天的威胁认知来看，我们将重要性的威胁拆解为几个维度：载荷（其中所使用的恶意代码和其他的软件工具）、行为（在主机上和网络上做了什么）、攻击方所使用的资源体系、攻击方所承载的攻击装备（攻击平台、载荷载具等）、攻击者是谁、攻击者的目的是什么、谁被攻击了、哪些资产被攻击了，以及对于相应的后果应该如何评价。这就是把传统的载荷检测、行为检测、信标检测转化为一个整体性的有依托的威胁认知。

用户的本质目的实际就是通过相应的检测与防御最后阻断攻击者的意图，达成保护自身资产的可用性、可靠性、完整性和保密性的目的。安天认为态势感知是围绕资产（即客体）展开的，其对资产的信誉、风险进行评估，对资产与威胁的关系进行揭示，对主体进行画像，对主体与客体进行关联。

### 4.3 支撑：“冰山”还是“大黄鸭”这是个问题

我们经常讲，一个优秀的网络安全企业应该是一个“冰山”，产品能力、服务能力都是水面上的部分，但是只有水面下的部分越庞大，也就是后端所拥有的支撑体系、数据体系和相应的人员组织体系越庞大，才能有效地支撑上面的部分。相对而言，当我们看到一个组织的全部能力都在水面之上时，我们相信其是一个“大黄鸭”型的厂商，这是一个不合理的结构，尽管看起来在水面上也有很多内容，但却是“风吹了就会被吹跑、针扎了就会被扎漏”的体系。

从我们自身的实践来看，安天在客户侧的引擎、产品体系、相关的服务所构成的有效防护、事件响应、资产监测和威胁情报的价值链其实是受到后面一个庞大资源体系的支撑的。仅仅通过地面部队的冲锋是很难有效冲破防线的，必须有后方强大的包括侦查、火力打击在内的全套支持。

### 4.4 建立应对安全问题的有效“敌情想定”

在当前网络安全实践中，感知能力未抵达关键目标内部，使得部署在真正的关键场景中的安全产品或感知手段变成了一种无支援的能力。这说明我们的网络安全缺少“敌情想定”，当前所采用的“物理隔离 + 好人假定 + 规定推演”，构成了最大的自我麻痹。物理隔离本身是一种重要的安全手段，但它不是安全的目的。物理隔离的当下实践，在一定程度上，是把安全能力的支援挡在了物理域的外面，却把对手放进来肆意为之，再加上假定内部都是好人，以及假定安全规定是完备的，使得人们认为对互联网开放资产的探测和可视化的叠加就是有效的态势感知。

总书记在 4.19 讲话中曾指出“物理隔离防线可被跨网入侵”。只有建立有效的“敌情想定”，才能使整个感知能力环节有效地向关键目标抵近，并建立起与整体态势感知平台的有效联系，才能最大化地降低隔离所带来的安全影响，发挥安全的支撑价值。一个合理的大系统安全规划应该基于：内网已经被渗透，供应链被上游控制，运营商网络的关键路由节点被控制，物流仓储被渗透劫持，关键人员和周边人员被从互联网侧进行定位摸底，内部人员中有敌特的人员派驻或被发展；要立足于战时高烈度对抗、平时持续性对抗，以及在平战中皆为无底线对抗和高成本对抗。

### 4.5 警告：态势感知不只是一种防御能力

态势感知不只是防御侧的能力，强大的攻击方也一直在建立相应的态势感知能力。比如，NSA 的 CamberDaDa 计划，是在 NSA 通过渗透他国运营商体系已经形成的前出监测能力中去挖掘其攻击目标与安全厂商之间的通讯，检查其中是否有相应的信息求助和样本发送，从而判断自身攻击是否暴露。对于攻防双方而言，无论是态势感知，还是人工智能，包括威胁情报，各种技术其实都是攻防双方的公共地带，从来都不是防御方所独有的垄断方法。

## 五、结束语

我们需要警惕的是，我们在万花筒里自以为看尽了世界，而对手却在阴影里用望远镜详细看着我们。安天人距离自身所追求的态势愿景依然有很大的差距，但是我们将不遗余力地去感知真实态势，做真态势感知。（因版面所限，文章图表未添加，可扫码阅读完整图文）