安天周观察

主办：安天　2018 年 01 月 15 日 (总第 120 期) 试行　本期 4 版　冬训营特刊　内部资料 免费交流

黑云压城敌情紧迫 红旗漫卷实战当先

——第五届安天网络安全冬训营首日纪实

2018 年 1 月 11 日、12 日，第五届安天网络安全冬训营暨关键信息基础设施保护论坛在哈尔滨召开。来自中国信息安全测评中心、国家互联网应急中心、中国科学院信息工程研究所、国家保密科研测评

第五届安天网络安全冬训营开幕现场

中心、哈尔滨工业大学等单位的专家，来自能源、电力、交通等行业的关键信息基础设施建设和运维专家与安天一起聚焦网络空间敌情分析，研讨关键基础设施保护新思路，分析实战化产品的达成。

本届冬训营主题为“敌情想定是前提，网络安全实战化”。安天在本届冬训营提出了以真实的敌情想定为前提，打破旧有以“物理隔离 + 好人假定 + 规定推演”构成的自我麻痹，让安全技术和能力转化为符合实战化要求的产品服务与解决方案，应对保障国家安全和发展利益的要求，为客户实现有效的安全价值。本届冬训营营语为“红旗漫卷”，在总书记十九大报告精神的指引下，安天将与客户一起向着红旗的方向前进，为保障我国关键信息基础设施安全构筑防线。

冬训营首日由安天研究院院长陈晓桦研究员主持，黑龙江省委网信办副主任孙耀武代表活动主办方致辞，中央网信办网络安全协调局应急检查处处长刘博、国家信息中心国信安全研究院副院长叶红等代表国家主管和相关部委致词。

■ 从自主可控到自主先进：建设网络强国的必由之路

中国工程院倪光南院士发表演讲

中国工程院倪光南院士进行了《构建安全可控的信息技术体系》的主题演讲，倪院士用详实的统计分析深入浅出地为大家解释了构建安全可控的信息技术体系的必要性。倪院士表示：“网信事业应当实施安全和发展同步推进。发展是硬道理，安全也是硬道理。”为了达到核心技术不受制于人，为了建设网络强国的需要，我国必须要构建安全可控的信息技术体系。倪院士同时还介绍了安天参与共同研讨的从自主可控到自主先进的安全举措：包括加强自主可控产品共有组件透明度、加强 IT 供应链的全程安全防护、加强产品证书的安全管理，完善自主产品漏洞补丁的分发策略、加强自主可控软件整体安全加固防护能力等。

■ 敌情想定：对抗安全威胁的核心前提

安天创始人、首席技术架构师肖新光发表了题为《网络空间的敌情想定分析》的主题报告。他介绍安天在 2017 年 6 月 2 日有关部门组织的关于“魔窟”事件的研讨会上，首次提出了“防御体系的建设需要以有效的敌情想定为前提”的观点，并提出要把“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

安天创始人、首席技术架构师
肖新光发表主题报告

制，物流仓储被渗透劫持，关键人员和周边人员被从互联网进行定位摸底”等作为常态化的敌情想定。

本次报告通过以对手的网络攻击作业能力体系为切入，分析了组织机构人员规模、预算投入，从信息采集和情报获取方式、装备体系、漏洞和恶意代码储备、系列支撑工程体系等多个角度进行了敌情分析。同时具体解读了不同国家背景的攻击者在端点、网络等方面的作业特点，并对比了不同能力层次对手的特点。

报告对比了“震网”事件、“乌克兰停电事件”、伪装成“必加 (Petya)”的攻击事件，指出了半定向攻击、“素人”式攻击等一些值得关注的新现象，以及“民间复合行为体”、“军工信息复合体”等新的活跃主体。报告分析了网络商业军火和高级军火泄露对网络空间命运共同体的安全威胁和地区平衡的影响。

（后续内容转第四版）

第五届安天网络安全冬训营次日图文纪实

为期两天的第五届安天网络安全冬训营暨关键信息基础设施保护论坛于今日落下帷幕。在两天的时间里，各位行业专家、学者以及安天的工程师们，分别从敌情想定及网络安全实战化的角度为大家带来了精彩的主题报告。第一天内容请参考《黑云压城敌情紧迫 红旗漫卷实战当先》；在此，小编对第二天的内容进行了总结整理，与大家一同重温精彩时刻。

■ 安天端点安全产品中心：《披坚执锐、决战终端防线》

端是安全之本，终端一直是威胁防御的主战场，面临着高级持续性威胁、勒索软件肆虐，传统杀毒的单点防护方式已经“力不从心”。安天智甲团队基于多年主机防御经验，立足敌情想定，在滑动标尺模型下，形成了从安全规划、被动防御、积极防御到威胁情报的层次化防御体系，依靠强有力的主防驱动、终端画像和群体防护模型。形成了能经受实战检验、可进行有效防御的终端安全产品。在终端的高烈度对抗中，安天将坚定以有效防护为目标，“披坚执锐，决战终端”。

■ 北京炼石网络技术有限公司创始人、CEO 白小勇：《商用密码技术在企业信息化中的实战化应用》

密码技术是企业信息化中实现数据安全的核心技术，尤其是在敌情客观存在的前提下。但目前，我们相对于商用密码的实战化还有一段距离。国产商用密码算法难以有效替换且不易于使用，使效率有所下降。

白小勇表示，基于以上问题，炼石网络对国产商用密码算法进行了相应的优化尝试，并得出，实战化的商用密码应用，就是在企业的关键信息化应用中，将密码能力适配进业务流程，输出有效的数据安全防护价值。

■ 北京上元信安技术有限公司 CEO 郑曙光：《“云”网络空间的威胁对抗与实战》

在报告中，郑曙光首先对以安天为代表的国内安全能力企业共同倡导的“网络安全滑动标尺模型”表示认可和支持，并将其与自身产品能力的结合进行了思考。借助被动防御与积极防御和威胁情报结合的理念，阐述为防御提供支撑的方式。

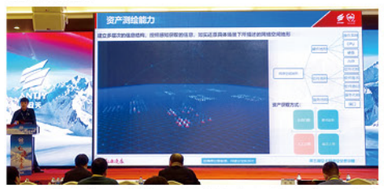
他表示，基于数据中心上云所遇到的安全困境，包括传统安全解决方案无法直接应用到私有云场景、私有云独特的安全风险急需有效解决方案等，上元信安提出了针对数据中心问题的解决方案，消除数据中心上云的安全障碍，提供不低于原有水平的安全能力，甚至可以提供新的防护手段和更高的防护能力。

■ 山石网科通信技术有限公司产品总监王中斌：《从微入手、层层防护》

王中斌以 Locky 勒索软件为例，说明在摸清楚威胁是如何一步步进入到内网中的情况下，采用针对性的防御措施和方案，以实现层层防御。

他表示，我们无法保住我们看不见的内容，因此，从微入手，针对敌情进行的可视化研究是所有威胁防御的基础，特别是在虚拟化环境中。在高级威胁防御方面，需知己知彼，针对高级威胁生命周期 kill chain 的不同阶段，应制定出层层防御方案。在内、外网多威胁防御方面，应认识到，“攻击都在外网，内网一定是好人”的假定在当前的网络安全中并不成立，需要有针对性的内网防御方案。

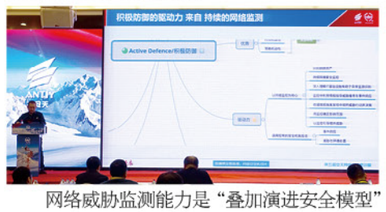
■ 安天监控预警产品中心：《态势感知全景能力构建》



来自安天监控预警产品中心的专家同事在分享中表示，态势感知是从微观、中观到宏观的，而非仅仅是宏观展示（即传统的地图炮）。态势感知应该是包含观察、理解、预测下一步动作以及响应和处置的上层体系化防御系统。态势感知的基础能力由扎实的基础能力构成。

面对飞速变化的威胁形势，安天始终立足于总书记实现“全天候全方位感知态势和有效防护”的工作要求，采用快速叠加演进的思路，构建真实有效的态势感知能力全景。“以敌情想定为前提”，实现态势感知在未知威胁发现与响应、基于资产的威胁发现与响应、情报驱动的威胁发现与响应等具体场景下的实战化应用。

■ 安天网络监测产品中心《智者伐道 -- 感知网络空间中的新威胁》



网络威胁监测能力是“叠加演进安全模型”中“积极防御”的驱动力之一，也是 OODA 循环的关键一环。在本次分享中，来自安天网络监测产品中心的专家以监测威胁（鱼叉钓鱼）、发现威胁滩头堡（水坑攻击）、切断攻击杀伤链（WannaCry）三个实战化的实例，从提升感知、持续检测、相应驱动三个方向介绍了如何通过人机结合充分利用网络威胁监测能力、实现感知网络空间中的新威胁。

■ 安天安全研究与应急处理中心：《潜伏的象群——来自某国的系列网络攻击行动》

2017 年 12 月 30 日，安天发布储备报告《潜伏的象群——越过世界屋脊的攻击》分析报告。报告对过去五年中中国遭遇的来自南亚某国此起彼伏的攻击进行了披露，并将具有相似线索和特点的一系列网络攻击组织和行动称为“象群”。

安天安全研究与应急处理中心（安天 CERT）对此进行了长期跟踪调查及分析总结。本次分享对“白象”组织及同样来自南亚某国的多个攻击组织的详细情况进行了介绍。我们应明确，在跟踪分析其所发动的 APT 攻击事件的同时，相关攻击组织也在不断进化和升级。在庞大的信息社会体系中，攻击面积大、可选择的攻击点很多，敌方可以很容易扩大战果。在这些攻击中，并没有高级 0day 和复杂的绕过技术，可见，只要不及时修订，就会有对手渗透进来，损害我国的国家利益，这就是“象群”给我们的教训。

■ 安天反病毒引擎研发中心：《下一代威胁检测引擎——对抗威胁实战》

传统威胁引擎立足于单纯的载荷检测而设计，以已知特征 + 部分未知检测模块的方式应对威胁。安天下一代威胁检测引擎立足于检测引擎可被获取并绕过的假想而设计，其为将鉴定器、识别器、拆解器、分析器等多种能力集合于一身的复合体。本分享以实际威胁检测、分析、追溯工作中遇到的问题为例，讲述了下一代威胁检测引擎在对抗威胁中的实战应用。

■ 安天安全运营中心：《锻造能力型工程师队伍，提供赋能式的安全服务》

安天在为用户服务、与威胁对抗的过程中，逐渐形成了解决用户安全问题的坚定信仰，不断沉淀对抗安全威胁的信念和勇气，确立安全厂商应具备的契约精神和价值观。2016 年，安天安全服务团队全面规模成长，其依托安天 18 年的技术能力体系和分析技术积累，依托安天监测处置产品作为利器，借力安天赛博超脑和态势感知平台，整合安天优势分析能力，锻造了一支能力密集型工程师队伍，专业服务于更多的客户，并将安天多年的经验积累赋能给客户。

■ 安天分析技术研究部：《基于密网的物联网僵尸网络监控与溯源研究》

物联网僵尸网络威胁利用 Linux 嵌入式设备的弱密码、漏洞入侵，获取百万量级肉鸡。Mirai 开源代码导致出现大量变种，国内黑产也利用其增加漏洞或交叉传播。安全专家通过蜜网可以捕获最新漏洞、攻击 IP、攻击资源和攻击者使用的恶意程序，监测 DDoS、垃圾邮件实时数据等。通过其绘制的 2017 年整体攻击态势可知，国外攻击者 C2 的存活时间大部分在 1000 小时以内，而国内 C2 则存活更久。

■ 安天安全研究与应急处理中心：《魔窟（WannaCry）事件的水面之上和水面之下》

安天在 2016 年网络安全年报中曾预测“勒索软件会与蠕虫的传播模式相结合”，结果不幸言中。2017 年 5 月 12 日，“魔窟”（WannaCry）勒索软件全球大规模爆发，我国大量用户受到感染。“魔窟”对全球企业、交通、金融，教育、能源甚至执法机构带来了严重影响。安天工程师回顾了 2017 年 5 月 12 开始近 30 个难忘的日日夜夜，介绍了分析“魔窟”蠕虫加密数据方法、分析数据可恢复性等响应点的经验过程，最后对标滑动标尺模型，分析了我方信息系统的问题现状。对“历史上的巨大灾难应以巨大进步为补偿”作出了期待。

冬训营落下帷幕，细粒度、针对性梳理敌情，加快网络产品服务实战化进程的工作更待加速。安天将与业内同仁共同携手，为建设网络强国一同踏上新的征程。红旗漫卷，长缨在手，勇缚苍龙！。

安天冬训营部分筹备组成员会后合影

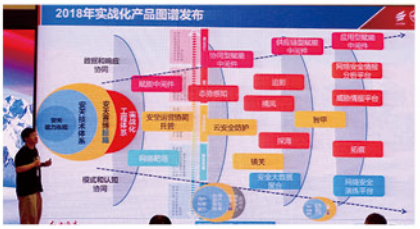
安天官方微博　　安天官方微信

报告结合了“白象”各攻击阶段所使用的漏洞和恶意代码，指出需要基于我方脆弱性历史分布和对手作业窗口进行叠加分析，不仅要进行脆弱性修补工作，而且要把对手在作业窗口期已经进入和预制作为一种既定事实。

报告提出需要以习近平总书记提出的“总体国家安全观”为指导，基于深度真实的对手分析，避免安全自我麻痹，建立敌情想定。报告重点解读了我国国防供应链安全所面临的安全风险和面临的敌情想定，并对比了自主 IT 产品生产、高科技成果研发、高等院校、民参军、遥感测绘、智囊智库等领域和场景面临的不同威胁意图、攻击入口和现状，提出敌情想定是针对性的、具象的。

肖新光呼吁按照总书记网络安全系列讲话的要求，充分认识网络安全的整体、动态、开放、相对、共同的特点，以相对性重新看待网络安全的策略设定和要求，将追求“绝对无损”的思维，转化为“有效防护、充分量损、快速止损、积极反制”的工作思路。立足于网络安全的对抗本质，对斗争的烈度、持续性、复杂性和变化性建立充分的认识。展开更系统、更具有场景针对性的敌情想定分析工作。

■ 实战化价值：安天 2018 年全新产品图谱发布



安天集团 CTO、安天移动安全 CEO 潘宣辰正式发布安天全新产品图谱

随后，安天集团首席技术官兼任安天移动安全负责人潘宣辰正式发布了安天全新的实战化产品图谱，并介绍了“赛博超脑”平台和相关合作理念。“赛博超脑”平台倡导以敌情想定为前提，打造网络安全实战化的产品，守卫新时代的网络安全。潘宣辰表示，安天将继续坚持网络安全的全能力布局，夯实基础工程化体系，持续扩大赋能型中间件（威胁检测引擎和安全内核）安全合作范围，结合云计算和人工智能技术，面向现实中网络安全防护的综合需要，构建实战化产品体系。向承担着关键信息基础设施防御使命的政企单位输出坚实可靠的安全能力，帮助客户全面落实网络安全的防御职责，使安全防御体系能够随时应对真实的威胁，实现有效的安全价值。

在会议上，安天还发布了《2017 网络安全威胁回顾与展望（征求意见稿）》供与会专家讨论。天津理工大学教授张健和神州网云 CEO 宋超在下午的会上分别发表了题为《新时代 新思想 新任务 – 加强我国关键信息基础设施保护》和《全流量的智慧漏洞挖掘》的报告，与会的专家学者共同探讨关键基础设施防护和网络安全的实战化问题。

安天作为引领威胁检测与防御能力发展的网络安全国家队，勇于承担对网络安全领域的责任，不断完善、创新自身的技术能力，为“服务客户、解决问题、应对威胁、保障价值”而努力，连续五届的安天网络安全冬训营从“凛冬将至”、“北风乍起”、“朔雪飞扬”、“冰峰屹立“到“红旗漫卷”，一如安天不畏险阻、不忘初心、永远在路上的团队征程。

中国工程院倪光南院士莅临安天参观指导

1 月 11 日下午，前来参加第五届安天网络安全冬训营的中国工程院倪光南院士莅临安天哈尔滨总部进行参观指导，安天副总裁王小丰做了介绍汇报。

在安天展厅，王小丰向倪院士介绍了安天的发展历程、现状以及技术分布，对安天威胁检测引擎的覆盖情况进行了说明。目前，安天的检测引擎已为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。在安天持续与网络安全威胁对抗方面，特别汇报了对高级威胁的发现、捕获、分析等方面所做的工作，重点介绍了安天针对“APT-TOCS”、“白象”、“方程式”等攻击组织的 APT 攻击情况、所使用的攻击装备及作业风格等方面的分析，以及对“魔窟”（WannaCry）等严重威胁的应急处理情况。倪院士对安天在恶意代码检测分析方面的持续投入以及与高级威胁的持续对抗上所做的工作表示肯定，并对安天威胁检测引擎的覆盖情况表示赞扬。

随后，他们来到安天反病毒博物馆，王小丰向倪院士介绍到，这相当于是安天的一个恶意代码文化长廊，其原来的目的就是为了在工程师上下班的时间起到一个学习的作用。在这面墙上，还预留了各位专家老师签字的地方，王小丰邀请了倪院士在上面签名留念。

在位于安天总部二层的安天安全研究与应急处理中心，倪院士观看了安天态势感知平台的演示，听取了安天对于建设国内多个态势感知项目的汇报，对安天为主管部门形成“抵近部署、集中感知、有效防护、快速响应”的创新思想和模式表示了赞赏，希望安天进一步推广。

最后，倪院士对安天的整体工作环境进行了了解，并与在场的工程师们进行了亲密互动， 倪院士在参观完安天图书馆、会议室及活动室后，对安天各处体现出浓厚的“工程师文化”氛围表示十分赞扬。