（上接第三版）

PC 场景到移动设备和 ICT 场景的完整技术栈。形成了围绕智甲终端防御系统、探海威胁检测系统、追影威胁分析系统、捕风蜜罐系统、拓痕工具箱的强威胁对抗产品体系。并投入近百人团队研发资产安全运维管理系统，以形成实时网空地形，打造态势感知基础底盘的目标；安天按照资产归属维度，将态势感知平台划分成监测型态势感知和战术型态势感知，并在国家网信系统、应急体系、关键信息基础设施行业，进行了打造高安全需求样板间的实践，其中四个项目入选了工信部网络安全试点示范项目。

▲安天威胁对抗核心技术栈

安天正在从支撑恶意代码对抗的小能力闭环，走向全面赋能客户、支撑客户，全面对抗威胁的大闭环。

聚力，塑造价值观与文化

“我是谁？为了谁？依靠谁？”，任何组织要达成基业长青，都要回答这一灵魂之问。习近平总书记指出“网络安全为人民，网络安全靠人民”，让安天人对所热爱的网络安全事业，有了更深入的理解，从最初“不懂网络安全的人是幸福的人，我们的责任是保卫他们的幸福”的质朴情感，到真正认识到客户是网络安全防御工作的主角，安全厂商是助力者、赋能者，重新理解了安全厂商与客户间的辩证关系。安天人以“智者 . 安天下”解读了自身的愿景，“智者”是安天的客户认知，安天人心中的智者，并非自己，而是客户。安天以客户为师，在赋能客户、服务客户过程中向客户学习，更好地达成有效安全价值。“智”是安天的方法认知，代表安天以创造性思维和工程化方法解决客户问题的工程师文化导向，以及提升安全保障的实战化和智能化水平的要求。“安天下”是安天的责任认知，代表着安天对客户责任、爱国主义责任和国际主义责任的理解与践行。

安天人确立了“不做与网络安全厂商价值观相违背的事情；坚持网络安全业务主航道不动摇；以网络安全为公器”的安天三原则，将“严守客户秘密”、“行为以客户授权为前提”、“进行负责任的信息披露”作为不可逾越的三条红线，赢得了主管部门、战略客户和生态伙伴的信任。

安天人以“达成客户有效安全价值”为使命，并希望进一步提升客户安全获得感、与客户共同探索提升对安全的认知。团队也形成了“正直、彪悍、专业、协同”的自身价值导向。

新起点，让历史告诉未来

安天以反恶意代码技术起步，十年技术实验室模式的探索，期间虽经历反病毒市场模式巨变，而依然以上游赋能授权模式执着前行；十年商业化转型，虽中途经历上榜外方情报机构重点关注名单，被迫退出美国市场的考验，但果断转型求变，走向政企市场，并站到了应对国家安全需求，对抗高级威胁的前沿。

从“能生存，不堕落”的创业六字方针，到打造“长寿而伟大”企业的对位校准。安天尝试出在一个窄带专业领域，通过“创新、使命、兴趣”单纯的理想主义驱动、依靠核心团队集体主义的自我压迫和奉献牺牲，将一个组织所能到达的价值极限。这一前期轨迹创新效率之高、坚持时间之长，都成为中国网络安全一条独有的模式与风景。这种坚持坚守也赢得了很多业内专家、同仁对安天的支持与帮助。安天人对此永远心怀感激。

创业早期，安天通过《团队宣言》，以“安天的一切权益属于为安天共同理想创造价值的人”表达对一个理想模式的理解；以“每一个人都是创业者，我们永远在创业的路上”，表达自身对创新与卓越的追求和拥抱变革创新的态度；并提出了“客户安全价值信仰、创业者公司、工程师文化”作为安天的三大文化基石。安天创业二十年之际，安天创始人明确提出“创业者共创共享的合伙人模式是安天治理结构的基础”，构筑安天百年发展的模式根基。

创业二十年，天地波澜壮阔，内心激情无悔。从信息化推动工业化到信息化带动工业化，安天目睹了中国发展变革和信息技术进步的伟大力量；从网络安全是信息化的配套保障，到“一体之两翼，驱动之双轮”，安天见证了网络安全战略价值的快速提升；从应对蠕虫木马到对抗高级持续性威胁，安天经历了从对抗普遍性威胁，到支撑国家安全，应对高级威胁的实战考验。

从引领技术创新潮流，到创造有效客户安全价值；从十年打造安全引擎，稳坐网络安全上游，到直接对接客户，承担赋能责任；从单一引擎赋能，到平台化、体系化价值输出；从核心团队自我牺牲，到创业者共创共享。安天自主创新的基因不改，承担国家安全需求的使命感尤为坚定，产品、服务、能力支撑系统不断强大完善，安天正在经历目标升级、模式自新、能力再造、机制重塑。

传承是最好的回忆，变革是最好的延续，胜利是最好的铭记。

2020 年 4 月，曾任中国电科集团三十所副所长、三十二所所长，并先后担任卫士通公司总经理，华东电脑董事长的游小明受到安天创始人肖新光邀请加盟安天，担任执行董事长兼首席执行官，与董事长肖新光组成了“光明组合”。6 月 6 日，安天成立二十周年，“光明组合”由新老安天人组成的新一届管理班底举行新征程誓师大会，他们中有安天联合创始人和资深专家；有来自央企和友商的高管；也有来自国家科研部门和国家运营商的科学家、资深的财经专家。新一届管理班子通过现场会议和远程视频向安天六地研发中心，十余个分支机构和办事处，面向近千名员工，分享了远景规划、组织设定、工作目标。

从今伊始， 迈向一个新的二十年征程就此开启。

2016 年 5 月 25 日，习近平总书记视察安天，对安天人作出了“你们也是国家队，虽然你们是民营企业”的重要指示，明确了安天的企业定位，提出了工作目标。安天新的管理集体将全面履行建设中国网络安全国家队的工作要求。

我们是安天，我们是中国网络安全国家队。

初心弥坚、征途尤远，浴血胜利，光明在前！

微信扫描二维码关注公众号

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 6 月 15 日 (总第 234 期) 试行 本期 4 版 创业廿载特刊 内部资料 免费交流

安天创业二十载，让历史告诉未来

铸核，自主创新融入团队基因

公元 2000 年 6 月 6 日是安天的创业起点。2000 年正处于个人计算革命的高峰与信息高速公路建设的一个历史交汇点。尽管在擅长的反病毒领域，安天创业者们一直是学习摸索的观察者，但新的场景可以让安天人越过 DOS 时代的窠臼，从全新的操作系统场景和万物互联的视角重新理解恶意代码，思考安全威胁的演进可能。在一无启动资金、二无客户关系背景，而同时又要坚守技术创新信念的情况下，安天人选择了一个独有的创业模式——技术实验室。“创造就是我们的脚步”的安天实验室就此诞生，以卡巴斯基为参照系，打造一流反病毒引擎和支撑体系成为了安天人的初始目标。时间是一切目标实现的代价，2000~2016 年，安天以十六年的时间，在基础引擎检测能力上逐渐追平自己的标尺企业；2010~2013 年，安天以三年的时间，在移动安全这个新战场上，打造了全球优秀的移动安全威胁检测能力。如果说创新是安天的基因；那么安全引擎已经成为安天的首个企业符号。为全球近百家网络安全企业、通讯设备企业、手机和智能终端企业、IoT 企业提供威胁检测引擎和相关安全中间件，累计覆盖超过 80 万台网络设备和网络安全设备、超过 17 亿部手机和智能终端。以关口前移的模式，支撑了一个良性安全生态。回望二十年，将安天部分创新工作进行提取，可以看到这样的一条轨迹：

安天在无启动资金、创业前十年拒绝风险资本注入的情况

（下转第三版）

▼安天创业 20 年的部分技术探索

时间	领域	工作	应多的威胁和场景变化	后续演进发展
2001	端点	扫描、检测、工具一体化端防 AGB	BO 等新型远控木马和 Rootkit 样本出现	智甲终端防御系统
2002	流量	骨干网恶意代码监测	网络蠕虫大规模爆发	探海威胁检测系统
2004	分析	批量样本自动化分析流水线	恶意代码数量激增	安天样本分析平台（VX-Plat）
	引擎	细粒度可嵌入的反病毒引擎	更多业务和设备场景产生恶意代码过滤需求	AVL SDK 威胁检测引擎
2006	端点	主机内核分析工具与四级授信	Windows 场景日益复杂，恶意代码分析难度增加	系统分析插件（ATool）
2008	捕获	用于恶意代码捕获的 ARM 载体蜜罐	强化扫描型样本获取能力，降低蜜罐部署成本。	捕风蜜罐系统
	分析	交互式集成分析工具	提高恶意代码分析效率，提升人工经验迭代	安全分析席位
	引擎	公有云化检测	规则库日益庞大，需要减少本地负载，需要增加可疑文件上报。	下一代威胁检测引擎（Cloud 接口）、赛博超脑云查杀服务
	引擎	多核 MIPS 平台的引擎支持	支持高速网络安全设备	AVL SDK 下一代威胁检测引擎（Network 版）
2009	分析	海量样本自动化分析第一代流水线	恶意代码数量指数级激增膨胀	赛博超脑分析子系统
2010	引擎	Payload Blocking	在控制通道和传输通道阻断威胁	AVL SDK 威胁检测引擎（for Network）
2011	引擎	移动反病毒引擎（安卓版本）	移动智能终端的普及势必带来移动端恶意代码的大幅增加	AVL SDK 威胁检测引擎（for Mobile）
2012	分析	恶意代码自动化分析第二代流水线	实现有效的人机互动。	赛博超脑分析子系统
	分析	沙箱前置化部署	将安全厂商领先的分析技术赋能给客户，同时保护客户敏感信息不外传	追影威胁分析系统
	引擎	私有云化部署的检测	客户敏感信息无法外传给安全厂商	智甲终端防御系统
2013	引擎	AVML 搜索	为分析人员对威胁的追踪溯源提供支撑	TID 威胁情报平台
2014	端点	虚拟化防护	传统反病毒产品不适应虚拟化环境	智甲终端防御系统（虚拟化版）
2015	端点	国产化系统安全防护	国产化自主可控趋势下的端点防护需求	智甲终端防御系统（国产化版）
2016	流量	流量侧全要素采集	满足高级威胁的分析溯源需求，且在五元组和全流量留存之间达成平衡	探海威胁检测系统（全要素版）
2017	引擎	下一代威胁检测引擎	构建攻击者难以预知的检测能力，并赋能威胁情报和态势感知	
2019	全域	全线产品支撑 ATT&CK 威胁框架	缺乏统一的攻击战术和技术定义及防护能力衡量指标	

每周安全事件

类 型	内 容
中文标题	研究人员发现 Stealthworker 恶意软件新活动
英文标题	Stealthworker botnet targets Windows and Linux servers
作者及单位	Pierluigi Paganini
内容概述	Akamai 的研究人员发现了一个恶意软件活动，该活动传播了一个用 Golang 编写的恶意软件 Stealthworker。该恶意软件针对运行流行 Web 服务和平台的 Windows 和 Linux 服务器，包括（例如 cPanel / WHM，WordPress，Drupal，Joomla，OpenCart，Magento，MySQL，PostgreSQL，Brixt，SSH 和 FTP）。Stealthworker 攻击者对在线暴露的计算机进行分布式暴力攻击，攻击者会对受感染系统执行有限次数的登录尝试，以绕过登录尝试次数的限制。一旦恶意代码破解出管理员密码，Stealthworker 就会安装和删除各种组件。
链接地址	https://securityaffairs.co/wordpress/104427/malware/stealthworker-botnet.html

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
活跃漏洞	Microsoft SharePoint 安全漏洞（CVE-2020-1024）	高	当软件无法检查应用程序包的源标记时，Microsoft SharePoint 会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。攻击者必须诱使用户将经过特殊设计的 SharePoint 应用程序包上传到受影响版本的 SharePoint，才能利用此漏洞。
	Microsoft Edge PDF Reader 安全漏洞（CVE-2020-1096）	高	当 Microsoft Edge PDF 阅读器不正确地处理内存中的对象时，存在远程代码执行漏洞。该漏洞可能以一种使攻击者可以在当前用户的环境中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。
	Microsoft Internet Explorer VBScript Engine 安全漏洞（CVE-2020-1035）	高	VBScript 引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。
较为活跃样本家族	Trojan/Win32.Reconyc	中	此威胁是是一种窃密类木马家族。该家族样本运行后会在系统文件夹中释放动态链接库文件和可执行程序，并设置消息挂钩函数，以获取系统相关信息并回传。
	Trojan/Win32.VB	中	此威胁是是一种使用 VB 语言编写的木马家族。该家族样本运行后会在电脑中下载其他恶意文件或未知程序，下载的恶意程序可能会远程连接其他网站，执行服务器脚本或下载其他恶意软件。
	Trojan/Win32.Blamon	中	此威胁是一种可以窃取密码信息的木马家族。该家族样本运行后会窃取用户账户信息，记录键盘击键等。
	Trojan/Win32.Fsysna	中	此威胁是一种木马家族。该家族样本运行后会在电脑的临时文件夹下释放恶意代码，同时添加注册表启动项，并发送网络请求。
	Trojan[Backdoor]/Win32.LolBot	中	此威胁是一种后门类木马家族。该家族样本运行后会在被感染的电脑中创建后门程序，下载其他恶意软件，允许黑客远程进入电脑窃取用户信息。该家族样本将自身隐藏在系统文件夹中，通常隐藏于应用数据的子文件夹中，利用 svchost.exe 进程，实现开机自启动并运行后门程序。
	Trojan/Android.SmForw	中	此威胁是安卓平台的一类木马家族。该家族样本运行后开机自启动，安装后隐藏图标，监听收件箱并删除接收到的短信，后台私自上传设备信息、短信、收件箱信息。且还具有远程控制功能，会造成隐私泄露，资费消耗，建议立刻卸载。
	Trojan/Android.Hqwar	中	此威胁是安卓平台的一类木马家族。该家族样本伪装成知名游戏应用，运行后隐藏图标，诱导激活设备管理器，接收短信指令，上传通讯录和信箱等隐私信息，进行发送短信、回复短信、拨打电话、卸载指定 apk、联网下载 apk 并弹出诱导安装等操作。建议立即卸载，避免造成隐私泄露和资费损耗。

（上接第一版）

下，通过打造高效威胁检测引擎和支撑体系的技术积累和成果价值，科技部 863 项目、发改委信息安全专项、科技部中小企业创新基金的支持。创业二十年，已申请专利 1087 项，获得专利授权 385 项，成为国家知识产权示范企业、获得国家科技进步二等奖一项、国家优秀发明专利奖一项、省部级科技成果奖五项、获得国际权威横向评测奖项，蝉联两届中国网络安全技术对抗赛冠军。并在 2015 年成为首个进入 CV500 网络空间创新百强的中国厂商，并在 2018、2019 年两度领跑 CV500 网络空间创新五百强上榜中国厂商，展示了自主创新的中国能力。

安天坚持对技术的开放与探索，从 2002 年开始，安天连续公开了基于流和包的病毒检测、骨干网恶意代码体系过滤的架构设计、细粒度可嵌入反病毒引擎、反病毒引擎的取证化应用等相关设计和技术细节，希望以“原创、沉淀、分享”的方式推动技术的共同进步，出刊 APT、移动安全、工控安全、热点事件等十个系列的安天原创技术成果分享 --《安天技术文章汇编》。

▲《安天技术文章汇编》

今天的安天已经成为拥有六地研发中心、两个省级工程中心、超过 800 名优秀工程技术人员的科创企业。尽管已经从实验室模式转型为科创企业模式，但安天研究院仍将承载安天基础与核心能力发展，坚守安天实验室的历史使命，安天也将延续新型研发机构的模式探索，在国务院黑龙江自贸区规划中，将由安天承建“哈尔滨网络安全实验室”。

塑魂，有效对抗威胁、支撑国家安全成为使命信仰

2000 年，以 Happy 蠕虫为代表的威胁泛滥的大幕刚刚拉开，以 Back Orifice 为代表的特洛伊木马也刚刚兴起。从 2001 年红色代码 II 蠕虫的捕获与分析开始，安天与应急响应结下了不解之缘，在第一时间捕获、快速发布分析报告和专杀工具，构造了应对蠕虫的模式样板。2001 年 4 月安天将病毒分析组改制为应急处理小组，并在 2007 年升格为安天安全研究与应急处理中心（CERT），并逐步形成了捕获、启动研判、信息上报、专杀 / 免疫工具、普查工具、报告发布等一系列标准动作，这套机制在支撑国家有关部门针对口令蠕虫、震荡波、冲击波、魔波、网络天空等流行威胁的响应、分析、溯源等工作中发挥了关键价值。

2010 年，是安天从实验室向企业模式的转型点，同样也是威胁演进趋势发生重大变化的转折点。2010 年 7 月，震网事件曝光，呈现出网空威胁对实体空间破坏的严重后果，威胁动机除了传统的心理满足和逐利外，更显露出国家行为体的狰狞面目。安天人快速搭建了模拟实验环境，进行了深度分析，陆续发布全面分析报告、相关技术细节验证、震网与毒曲同源性等分析成果，安天人将分析工作重心逐渐转入到以国家 / 地区行为体为背景的高级威胁中。2013 年安天依托分析报告扩线，发现了白象攻击组织对中国高校攻击，并成功画像到组织，溯源到自然人。2015 年 5 月 27 日，安天发布报告（点击查看），明确指向某国攻击组织对我国政府机构攻击，并发现其使用了商用攻击平台 Cobalt Strike；2013 年 ~2019 年，安天针对能力最强的 NSA 下属的方程式攻击组织进行持续跟踪分析，取得了破解木马远控通讯加密机制、深入分析固件持久化机理、拼接出模块化木马拼图等成果，特别是在 2019 年 6 月，安天发布长篇报告（点击查看），完整复盘 NSA 攻击中东最大金融服务机构的全过程。在这些工作中，安天 CERT 作为安天核心应急和深度分析力量，不断成熟，逐步形成了“第一时间启动，同时应对两线威胁，三体系联动，达成四作业面效果”的工作机制，形成了对近 300 个攻击组织的持续跟踪画像能力。安天也连续六届十二年蝉联国家级网络安全应急服务支撑单位。

铸器，构造威胁对抗能力系统

2000 年，安天的初创者们构想了一套 ArrectNet 预警监测体系，这个体系由主动上报、诱饵信箱、捕获三个环节组成，这个想法的初始实践是和 IDC 在少量主机上安装系统环境监测程序的合作，这一思路很快在 2001 年捕获红色代码 II 中发挥了重大价值，而后历经捕风计划（蜜罐，2004 年）、探云计划（流量，2006 年）、猎狐计划（网站，2008 年），安天逐步建设完善了一套立体化的威胁监测机制。也为后来推出捕风蜜罐系统、探海威胁检测系统奠定了产品基础。

▲ArrectNet 监测捕获分析体系在 2006 年的结构图

2001 年，在国际知名反病毒企业在南亚大规模的招聘数以千计的分析工程师的时候，安天提出了“自动化分析流水线”的想法，并通过“短特征加权”、“成分分析法”等方法进行尝试。2004 年，随着第一代分析平台上线，安天初步实现了全量恶意代码威胁自动化分析，并尝试将决策树、沙箱分析等先后应用于分析平台。安天通过 XML 格式自定义的 AVML 格式，形成对海量非结构化分析数据的关联与存储，通过在 2013 年建构 AVML 搜索系统，形成安天 ATID 和 AVL Insight 威胁情报系统的雏形。

这一整套从威胁捕获到分析的系统，尽管只是为了支撑恶意代码对抗这一窄带目标。但其成为了安天对网络安全态势感知基础的早期实践和自我积累，为安天后续承担大量国家机构和战略客户的态势感知平台建设打下了基础，也成为了安天赛博超脑支撑体系的基础。

而安天在实验室探索阶段研发的 Antiy Ghostbusters 反木马工具，ATool 系统安全处置工具等，在历经多年维护发展后，也演进为安天智甲终端防御系统和安天拓痕工具箱。

安天通过二十年的努力，构筑了一套包括从核心引擎到大规模自动化分析体系；从端点系统安全到流量安全监测；从传统

（下转第四版）