安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 02 月 05 日 (总第 123 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天技术体系与产品图谱

我们的主题是安天作为一个能力型安全厂商，希望采用何种方式践行能力布局、形成技术体系、主导产品研发，以达到实战化效果的过程。一些商业公司在讲自己的技术体系和产品时，通常是以商业愿景的视角作为前提和判断依据。而安天的基础认知角度则是**以网络安全对抗核心诉求为出发点形成能力布局，在此基础之上建设所需要的安全核心技术体系，并最终推动整个产品的设计和相关研发**（图 1）。

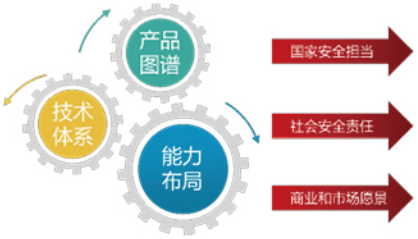

图 1 安天对网络安全的基础认知

2000-2012 年，安天一直是一个偏于上游供应商风格的网络安全厂商，自 2013 年开始，逐步转向前台化。由于整体的研发和技术体系的思考模式和价值观的不同，安天在做相关安全产品时会相当克制，不会贸然去做大量形态不同的安全产品。安天其实是从能力布局、技术体系到产品图谱的角度去思考，综合性地考虑要承担什么样的国家安全担当，肩负什么样的社会安全责任，并且如何平衡好一个民营企业应该具备的商业和市场愿景，以及在市场上应该扮演什么样的角色。

能力布局和持续对抗意图的演进

安天对于网络安全企业能力的思考是有一段演进过程的。2000 年，安天以当时的核心对抗聚焦点恶意代码为切入点；之后透过蠕虫的规模化传播现象，安天认为

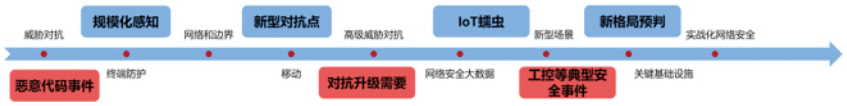

图 2 安天对于网络安全企业能力思考的演进

基于网络威胁流量探测构建规模化的感知能力是必备的核心能力；而随着木马的规模化增长，蠕虫的规模逐步降低，安天发现规模化增长的木马必然需要驱动整个后端的工程化体系；再之后，安天看到了移动这种战略级、产业级新型对抗的卡位需要，看到了高级持续性威胁（APT）所带来的对抗升级的需要，看到了新的物联网时代以及工控场景下的安全形势，包括对当前新格局的预判和敌情的重新认知，面对这些认知，安天都有目的性的展开了能力布局的设计和投入（图 2）。

可以看到，这个过程既包含提前性的能力预判，同时也伴随着形势和当前突发型安全事件所带来的新安全认知的综合迭代，安天对安全的不断认知和对威胁对抗的持续思考从始至终贯穿其中。

以对抗为前提架构技术体系并支撑产品规划

能力布局的演进思考经过了十几年的迭代、优化、归一化以及重新调整，以此为基础，我们再真正展开内部的技术体系和相关工程化支撑需求的落地。从大家最熟悉的安天最早的反病毒引擎，到后来的终端防御产品，我们认为**终端始终是一个与安全对抗的一线和终极产品，如果没有相关技术去达到对抗实效，其实无法支撑一个能力型厂商对产品的定义和需要。**

后续也有其他技术体系被逐步建立起来，所有这些技术体系中都有比较关键核心的对抗环节，例如对于恶意代码的识别和判定、对于流水线的分析和支撑、对于网络规模化的检测，以及包括像移动和新兴场景带来的整个平台的基本工程化思路和体系的创新需要。在不同的技术体系背后，同样有对应的工程化体系支撑，这些工程化体系之间会有相关的叠加和演进，也有跨平台的革命性创新和迭代。**而当出现了更高级、更立体、更综合性的威胁需求时，就需要呼唤整个体系的一体化横向打通，以实现对更高级的威胁对抗场景综合立体的工程化支撑**（图 3）。

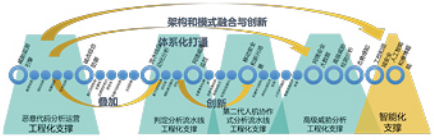

图 3 安天以对抗为前提的架构技术体系

2000-2008 年，安天的产品化和研发本质上还是以工程师自身的应用为视角来进行专业型产品的创新。不论当时还是现在，安天都适当放弃了对合规型需求的研发投入和支持。从最早的引擎 SDK 到相关桌面型产品的尝试，再到 2002-2003 年，安天在国内很早开始做的自动化的沙箱、流水线分析系统、旁路的威胁规模化监测等，可以说在此阶段，安天的产品确实是一种比较技术理想化的工程师视角尝试。而这些尝试所带来的不良后果，在安天的商业能力对于技术体系和能力体系的投入达到一个不平衡情况的时候开始突显。所

（后续内容转 2、3 版）

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有9个移动平台恶意代码和4个PC平台的恶意代码值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	G-Ware/Android.Xiny.a[exp,rog] 2018-01-31	该应用程序植入恶意代码，运行后上传用户固件信息，加载广告，私自下载其它应用并诱导安装，造成用户资费消耗和隐私泄露，建议卸载。（威胁等级低）
		Trojan/Android.shenyouspy.a[prv,spy] 2018-01-31	该应用程序为微信工具，运行后会监听短信信息并上传到指定网址，同时会获取用户的QQ好友数量以及微信好友数量进行上传，可能造成隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.LockerAds.a[exp,rog,spr] 2018-02-01	该应用伪装成壁纸应用安装器，运行加载子包，下载流氓广告插件，后台频繁推送广告，造成用户资费损耗，建议卸载。（威胁等级高）
		G-Ware/Android.INSIDE.a[rog,pay] 2018-02-01	该应用程序伪装密室逃脱论坛应用，私自安装子包，子包远程下载安装诱导用户付费的游戏应用，后台推送广告，会对用户的资费造成一定的损失，建议卸载。（威胁等级中）
		RiskWare/Android.FakeEWallet.a[fra] 2018-02-01	该应用程序非官方应用，运行后推广虚拟货币交易平台，虚假电子钱包，可能造成财产损失，另外还会加载广告，请谨慎使用。（威胁等级低）
	较为活跃的样本	Trojan/Android.Smstracker.e[prv,rmt,spy]	该应用程序安装无图标，接收短信控制命令，后台窃取用户短信、私自录音、私自拍照，并将这些用户隐私信息通过邮件发送至指定邮箱，造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.Hellospy.b[rog]	该应用程序开机自启动，运行后隐藏图标，定时启动恶意程序，与其他程序组合造成危害，建议卸载。（威胁等级中）
		Trojan/Android.AJEJE.b[rmt,prv,spy]	该应用程序伪装成系统应用，运行后隐藏图标，接收远程指令开关手机移动流量网络，上传用户社交应用隐私信息，更新安装指定应用，还会将该应用写入系统保护程序，防卸载，会造成用户隐私泄露，建议卸载。（威胁等级高）
		G-Ware/Android.Hiddad.d[exp,fra]	该应用伪装成系统升级程序，无实际功能，包含google广告插件，运行即隐藏图标并加载运行广告模块，会造成用户一定的资费消耗，建议卸载。（威胁等级低）
PC平台恶意代码	活跃的格式文档漏洞、0day漏洞	Microsoft Office 远程代码执行漏洞 CVE-2017-8570	CVE-2017-8570漏洞是一个逻辑漏洞，该漏洞和SandWorm（沙虫）漏洞类似，因此被称之为“沙虫”二代漏洞。该漏洞为Microsoft Office的一个远程代码执行漏洞。其成因是Microsoft PowerPoint执行时会初始化ScriptMoniker对象，而在PowerPoint播放期间会激活该对象，从而执行sct脚本文件。攻击者欺骗用户运行含有该漏洞的PPT文件，导致获取和当前登录用户相同的代码执行权限。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/HTA.Locky	此威胁来自一类可以下载勒索软件的木马家族。该家族样本是Html Application应用程序，运行后连接远程服务器下载Locky勒索软件并执行，加密用户重要数据。（威胁等级中）
		Trojan[Downloader]/Win32.Paskod	此威胁来自一类可以下载恶意代码到本地的木马家族。该家族样本运行后连接网络下载恶意代码并执行，可能会收集用户信息并回传。（威胁等级中）
		Trojan[Rootkit]/Win32.Crypt	此威胁来自一类可以窃取用户信息的木马家族。该家族样本运行后可以下载并执行其他文件，连接远程服务器发送自身信息，关闭系统防火墙，有一定威胁。（威胁等级高）

（上接第一版）

以自2009年开始，安天选择了一次对产品线的整体收敛和回收，仅仅保留了当时安天最熟悉的和最擅长的已建立了业务基础的供应链赋能型产品。这些产品在2005-2006年取得了防火墙供应链能力的突破并以此为基础在2008-2009年才促使安天决定要在移动互联网产业发展初期提早布局这种模式。这次产品线回收一直持续到2013年。而下一个阶段则是2014-2017年，安天在此阶段采用新的思路来重新尝试专业型产品，而此时国家已经空前重视网络安全，包括用户以及行业内也开始大力推动技术和产品创新，甚至市场需求也已经开始逐步从合规型驱动慢慢向专业型和技术型驱动转变。越来越多的网络安全厂商、创业企业开始注重技术创新和专业型能力输出，这种情况所带来的问题是现实的市场中可能会出现越来越多的技术名词、产品功能名词、热词，我们好像看到了很多美国创新的故事、创新的能力以及概念开始大规模出现，但这种演进过程我们认为是完全不够乃至泡沫的，甚至可能很多用户场景和实际场景与网络安全对抗的一些规律和特点是相违的。

2015年，Seak最早提出了“**赛博超脑**”的设想，其**本质是可以在内部所有技术体系背后的工程化支撑体系基础之上，实现跨工程化体系的架构和模式上的融合和创新**，在此基础之上，我们不仅希望这种智能化的支撑体系可以结合现在的云计算、人工智能等新的技术应用思路，去达到内部工程化体系融合的效果，同时也希望能够通过这种新型的平台化的建设，去把原来我们和客户的合作关系以及安全能力的输送方式进行调整和改进。目前我们已经在移动场景逐步建立了对于云计算、大数据、人工智能的技术应用，安天已经经历

了从每年保护百万级终端，到每年保护近十亿部终端迭加演进的过程。这些都为赛博超脑设想在基础架构的需求上做出了最扎实的技术和工程储备。

以全能力布局和核心技术体系支撑实战化产品体系

当前我们所做的一些工作是不够的，前提是有问题的，一旦当安全前提和假设出现问题，之后其实是在用非常正确和高效的过程去做一个前提错误的事情，最终的结论一定是安全防御的失效和陷入安全的自我麻痹状态。所以在我们做安全产品的时候，在做最终安全投入落地的时候，还是要回归到敌情前提，去客观考虑、结合安全现状，重新从实战需求有效落地的角度去考虑产品。

安天从 2016-2017 年开始对产品进行持续深度思考，并在 2016 年和国内其他能力型厂商联合引进了由美国相关机构创立出来的类似于“滑动标尺”、“OODA”（观察 -Oberve、调整 -Orient、决策 -Decide、行动 -Act）对抗认知迭代模型，并将其引入到国内的一些安全产品及解决方案和服务的一些输送过程中。在此过程中，我们看到这种方法和工具是具备积极效果的，但同时它需要和中国国内防御环境中的真实用户需求和安全需求重新进行结合，而此过程是需要破掉许多我们之前错误的前提和假设的。这个“破”的过程，其实是回到一个比较客观和符合规律的网络安全现状认知的过程。

安天在思考自身的产品体系到底应该具备什么样的差异化价值和竞争力的时候，最开始想到的是可以操作化、脚本化、可运营化，并建立持续性，其本质并不是从复杂的技术概念或角度去讲我们如何能持续有效，创新的技术在有效面前还是有一段距离的，而**真正的有效往往是从最基本的 What（什么前提、什么假设）、Do（我们应该做什么）、Who（谁应该做什么）、When（什么时候做什么）、Check（做了之后还要检查什么）、Why（这些事情为什么是有效的）开始，以重复大量的基础简单事务来构成一个基础，在一个正确的前提下，才能综合累加出一个有效的实战化的安全防御效果。**习近平总书记在视察军队时多次提出“着力提高部队实战化水平”、“着力深化实战化军事训练”的要求。**网络空间安全事关国家安全，更应该以实战化为基本要求，才能有效应对网络空间战场上持续不断的高烈度无底线较量，而实战化必须以有效的敌情想定作为基础和前提，只有更了解对手，才能更好地保障客户的网络安全。**

我们所看到和理解的实战化，**本质就是如何根据自身的产品能力和功能，去面向实战的需求，在定制和开发的过程中，形成一种真正结合客观网络安全现状认知的综合性布防的效果。**在这种布防形成的战术前提之下，告知安全人员、组织和决策者，应采用怎样的方法和理念，去增加人员和投入，并指定相关的角色和职责；告知相关人员采用怎样的战术和策略，并明确操作细节，以达成一个真实有效的实战安全能力的目的。而在最终的产品实战化的输送中，应该是由产品的基础架构，到持续完成对抗认知的迭代，再到通过类似于滑动标尺和其他相关的用户有效性或者安全输送能力层次，以及有实战检验策略的工具，逐步完成和用户交付的过程。

安天 2018 年实战化产品图谱

安天对于下一个大阶段产品的思考所做出的一个具象化的考量就是“实战化”。在此基础上，我们根据长期的实践积累推出了新的产品图谱（图 4）。**我们将从安天原有的产品布局和技术体系，重新面向实战化的客观需求去定义完善产品架构，并通过安天的内部平台把其转化成一个真正可以去支撑实战化的智能体系。**这个智能体系的支撑平台就是赛博超脑平台，以它为支撑将有 2 条能力延展线路，一条是原有的安天的赋能产品体系，实现设备协同体系的赋能、供应链嵌入式赋能、应用场景的细粒度赋能，达成数据和协同层面的联动；另外一条是通过以“赛博超脑”为基础构建服务型平台，帮助行业和特定用户群体，建设具备私有化能力、私有化架构和私有化实战指挥中心的安全大脑，以及在各个端点和边缘上尝试建设具备私有数据、私有检测、防护和处置能力的安全小脑，达成一个模式和认知的协同。而在中轴，会以滑动标尺或者相关有效的认知对抗模型工具为指导，构建不同层次的产品体系。

在此过程中，安天将会在既有的态势感知、追影、捕风、探海、拓痕等产品基础之上，弥补相关核心产品盲点，并基于在安天既有的海量移动终端基础上形成的安全大数据的聚合以及相关威胁情报和网络安全情报平台，实现更全面的产品布局。最终，安天将通过立体化安全服务和解决方案体系，来实现对于整个实战化产品的对外输出。希望通过这种方式，能够将有效防御能力真正赋予到所有的用户和防御侧，在真正使用安全产品的人员、设备上达成安全价值的有效落地。

图 4 安天 2018 年实战化产品图谱

自 2018 年起，安天会在未来几年时间内，不断践行安全产品的实战化理念。自我加入安天已经有十年的时间了，我心中的安天和我看到的安天一直是一个有着战士般使命、担当和意志的厂商。在安天发展的过程中会出现一些问题、错误和软件的不成熟，一些用户很认可安天，但也会指出安天产品上的不足。针对这些问题，安天一直都非常虚心和诚恳地去认同这些不足，探讨这些不足，积极面向实战的方向去演进和改进。非常感谢大家能够认可安天，希望可以和大家一起共同践行和尝试网络安全实战化，就像习总书记说得那样，当前已经是一个新时代了，希望可以用这种姿态和大家一起去守卫这个新时代的网络安全，也揭开一个网络安全的新时代。

——本文依据安天首席技术官潘宣辰在第五届安天网络安全冬训营上的演讲整理而成。

安天发布《inetinfo 家族样本分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时发现一例后门样本，名为“inetinfo”。该样本利用 445 及 3389 端口实施恶意操作，获取用户网络信息并通过邮件回传，可以猜测该恶意代码为某攻击的前导样本。

该样本是一个后门程序，该样本会根据参数个数以及参数内容进行不同的操作。如果参数个数不为 1 或者参数不是 45 则为程序中的服务提供 ServiceStartTable 结构，其中包含服务名称 RdpCertification 和服务主函数指针。如果参数符合要求，则根据参数的值来进行相对应的操作，如创建服务、删除服务、开启服务以及执行服务主函数等操作。服务主函数的功能是测试本机所处的网段中 445 端口以及 3389 端口是否可以使用，若可以使用则连接“本机所处网段：445”获取账户信息，连接“本机所处网段：3389”发送邮件。随机生成 IP，测试 IP 所处的网段的其他 IP 是否可以连接，若可以连接则连接“IP：445”获取账户信息，连接“IP：3389”发送邮件。通过获取到的邮件了解受害者网络拓扑信息，这样攻击者就可以确定可以攻击的目标，准备下一步的攻击。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来演是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。目前，安天追影产品已经实现了对该类恶意代码的检出。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 YARA 自定义规则鉴定器、数字证书鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据智能学习鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	system32_inetinfo.exe_
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	84 KB
MD5	6D94E3B273D3DADA89ECCA6C48A4F577
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.Joanap.A!dha
判定依据	智能学习
下次鉴定时间	约 2 周
首次发现时间	2018-01-02 09:57
末次发现时间	2018-01-31 09:42

◆ 运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 文件元数据分析

File Size	84 kB
File Type	Win32 EXE
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
Time Stamp	2017:08:07 14:24:08+08:00
PE Type	PE32
Linker Version	6.0
Code Size	20480
Initialized Data Size	61440
Uninitialized Data Size	0
Entry Point	0x560c
OS Version	4.0
Image Version	0.0
Subsystem Version	4.0