安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 11 月 26 日 (总第 161 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天负责人：以全面能力导向建设模式带动网络安全需求解放

本文转载自《中国信息安全》

一、网络安全产业发展赢得了空前的历史机遇

当前，我国网络安全的顶层设计逐步完善，工作要求明确。全社会对网络安全重要性的认识不断提升。网络安全产业迎来了前所未有的发展机遇，而产业发展的关键在于将战略判断和认识转化为硬性的工作要求，转化为有效的工作落实，从合规检查、应对单点威胁为驱动，走向全面能力导向建设的模式，充分解放需求。

习近平总书记的系列讲话对网络安全工作效果要求不断提升，为网络安全能力建设指出了方向。2016 年的“4·19”讲话要求“全天候全方位感知网络安全态势”，对态势感知提出了增强连续性、抗干扰性和无死角的要求。此后，在 2017 年的“2·17”讲话中，总书记将工作要求提升为“实现全天候全方位感知和有效防护”，要求改变无效防护的局面，从感知风险的存在，提升至通过有效防护对抗威胁、控制风险，并强调了感知与防护能力必须做到全方位覆盖。在今年的“4·20”讲话中指出要“关口前移”，对落实网络安全防护的方法提出了重要要求，而“防患于未然”则形成了鲜明的以防护效果为导向的指引要求。

二、防御能力缺失导致的无效防护问题依然严峻

通过安全监测、防护和处置工作看到的情况是，有大量信息系统还处于“缺感少知或虚假感知”、“缺少防护或无效防护”的状态，距离总书记“全天候全方位感知和有效防护”的工作要求还有相当大的差距，“防患于未然”就更难达成。“物理隔离 + 好人假定 + 纸面推演”形成了自我麻痹和虚假安全感，面对勒索蠕虫这样低层次的非定向攻击，很多重要信息系统内网、关键信息基础设施，出现了大面积感染情况，这样的防护水平显然不能防范有国家和政经集团背景的高级网空威胁行为体的攻击。从安天监测分析的“白象”、“绿斑”、“海莲花”等高级网空威胁行为体的攻击来看，多数攻击中频繁使用的是陈旧漏洞。这种攻击方式能够起到作用，正是因为防御能力的不足为对手提供了攻击敞口，暴露了长期投入不足、能力建设的驱动力不足导致的防护缺失。这种防护缺失并非只是技术先进性不足的结果，而是信息系统在规划建设运维中，未能同步考虑网络安全问题的结果。在架构安全、纵深防御、态势感知与积极防御、威胁情报等层面都存在能力缺失、离散建设和碎片化投入等问题，十分严重。

网络安全能力不能适配保障网络强国战略目标的实现，是当下严峻的问题和挑战，如能直面问题，迎难而上，则又正是把握信息化跨越式发展的重大历史契机。做好网络安全防护工作需要以客观敌情想定为前提，按照应对敌情的标准进行高线能力建设。一个国家的网络安全防御能力最终是由攻击者和窥视者检验的。客观的敌情想定是做好网络安全防御工作的前提。在当前激烈的大国博弈和地缘竞合的背景下，具有国家和其他政经综合背景的高级网空威胁行为体，对我国重要信息系统、基础设施进行入侵渗透，形成远程控制、情报窃取能力，预谋实施干扰、破坏、毁瘫等，已趋于常态化。能否有效防御这一层次的攻击，对于维护我国主权、安全和发展利益，非常重要。

在信息化、网络化发展的初期，我国依靠合规驱动、评估检测等手段，逐步推动了网络安全制度规范、技术环节从无到有，形成了基础及格线要求。在社会发展运行高度依赖信息化的今天，重要信息系统和关键信息基础设施的防护，如果连合规标准都不能达成是注定不行的，但是仅仅达到合规要求也是远远不够的。需要深入分析对手，建立完善“敌情想定”，按照应对敌情的高线为标准进行安全能力建设。应以“敌已在内，敌将在内”作为研判的基本前提，充分认清信息资产特点和防护需求，充分考虑供应链、外部信息环境、信息交换、人员社会关系等方面的综合挑战，结合对敌情想定中各攻击、关联方的国家战略、作业意图、攻击能力、作业风格、装备体系等进行对标分析，才能有的放矢。只有将重要信息系统和关键信息系统防护目标从符合合规标准，提升到应对“假想敌”的防御水平，才能改变防御缺失的现状，形成真正意义上的有效防护。

三、以系统性的能力导向建设模式牵引需求解放

“网络安全的本质在对抗，对抗的本质在攻防两端能力较量。”无论是核心技术突破、产品功能深化，还是产业体系发展，网络安全领域所有进步和发展，都要转化为防御场景下的实际能力，经历实战检验。从发达国家网络信息安全建设规划发展的经验来看，也经历了从合规导向建设模式到威胁导向建设模式，在 21 世纪初就已经逐步走入到能力导向建设的模式。

美国国防部 2001 年《四年防务评估报告》中指出：随着冷战结束，国际形势日益复杂化，已经很难清晰地识别出所有的敌对威胁行为体，因此需要从基于威胁的规划模式转为基于能力的规划模式……需要把尝试罗列各种可能的网空威胁并设计零散防御措施进行被动应对的传统式威胁导向建设模式，演化为全面建设必要的网络安全防御能力并将其有机结合形成网络空间安全综合防御体系的能力导向建设模式。

下转第二版

上接第一版

2002 年，美国推出了《联邦信息安全管理法案》（FISMA）。FISMA 在充分认识信息安全对于美国经济和国家安全利益重要性的基础上，要求各联邦机构制定并实施适用于本机构的信息安全计划，保障联邦信息和信息系统安全。

在 FISMA 的牵引拉动下，美国联邦政府的安全预算在 IT 总花费占比得到提升，并在奥巴马执政期间形成一轮能力建设高潮，在 2012 年一度占比达到 19.5%。

如果希望网络安全形成规模型产业，就必须形成高质量的规模化需求。我国在网络安全法颁布实施、网络安全责任制大力推行的背景下，未来将会迎来网络安全投入建设的高潮。而相关投入能否有效转化为综合防御体系能力，并不能简单地靠增加投入来完成。网络安全既需要资金投入保障，同样也需要能力导向的安全规划与建设。在网络安全投入中，需要推动架构安全、纵深防御、态势感知与积极防御、威胁情报的能力建设叠加演进，形成示范方法和最优实践。

一方面，要对现有的关键基础设施等提出应对“敌情想定”的更高防护，另一方面，新兴智慧城市、工业互联网等信息化的增量建设部分，更积极地落实总书记关于“安全与发展同步推进”的工作要求，在信息系统规划、建设、运维的全生命周期中都考虑网络安全问题。在新一轮信息化加速投入，拉动经济社会发展过程中，实现网络安全能力的深度结合与全面覆盖。

四、产业发展需要切实的金融、财税政策支持

网络安全产业发展，需要进一步的市场、金融、财税政策的支持。各行业领域的历史发展经验证明，直接给钱补贴的方式，不是一种最优的模式，而是需要同时激发供给和需求两端。一方面，需要建立优胜劣汰的市场规则，将支持创业发展、技术自主创新的政策对网络安全企业落实到位。另一方面，更需要有利于释放需求，提升政企机构网络安全投入积极性的激活需求侧举措。如能将网络安全建设投入作为企业税前加计扣除，将经济落后区域的网络安全投入纳入中央转移支付项目，就是一种推动需求的策略。

在“一带一路”国家和友好的第三世界国家中打造、提供更多网络安全援外项目，这不仅是推动产业发展，也是中国为保卫网络空间人类命运共同体承担的国际主义义务。

中国网络强国需要网络安全产业能力支撑，网络安全产业则需要规模化发展。“历史只会眷顾坚定者、奋进者、搏击者，而不会等待犹豫者、懈怠者、畏难者。” 战略挑战和战略机遇都摆在中国网络安全产业人面前，我们需要给出自己的答卷。

（本文部分观点参考了黄晟同志为即将出版的《网络空间安全防御与态势感知》一书所作的译者序，特此致谢。）

注：

《肖新光：以全面能力建设导向带动网络安全需求解放》文中，误将“能力导向建设”，写成了“能力建设导向”，此系作者笔误所致，特此更正，并向杂志社和读者表示歉意。同时，已在转载过程中做了相关修改。“能力导向建设”强调的是能力完备性和运行模式演化。

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 6 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

关注方面		名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.seafko.a[prv,rmt,spy] 2018-11-16	该应用程序伪装系统服务，运行隐藏图标，后台接收远控命令，窃取用户短信、联系人、通话记录、位置等隐私信息，私自录音、拍照、发送短信等，会造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.FlokiSpy.a[prv,exp] 2018-11-17	该应用程序伪装正常应用，运行隐藏图标，联网上传短信信息及用户手机相关信息，并私自转发短信至指定号码，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.congCS.a[prv,sys,spy] 2018-11-19	该应用程序伪装系统服务，运行后隐藏图标，释放提权文件私自提权，窃取用户短信、联系人、浏览器记录、地理位置、社交软件信息，静默安装未知文件，私自拍照、录音，并上传至服务器。造成用户隐私泄露，建议立即卸载。（威胁等级中）
	较为活跃的样本	G-Ware/Android.Ruok.a[prv,exp,rmt,rog]	该应用程序伪装正常应用，运行隐藏图标，联网接收远程指令，上传应用安装列表、固件信息，下载未知应用，访问推广界面，造成用户资费损耗，请卸载。（威胁等级中）
		Trojan/Android.FakeUVC.a[prv,rmt]	该应用程序经过篡改处理，包含恶意代码，后台接收远程控制指令，窃取用户短信、地理位置、手机图片等隐私信息，私自拍照、录像，私自发送短信，并将隐私信息上传至服务器，造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.AccmediaSpy.a[prv,rmt,spy]	该应用程序伪装系统组件，实际为间谍件。运行诱导用户授权，隐藏图标，后台联网接收远程指令上传用户联系人、信箱、地理位置、通话记录、录音、照片、SD 卡存储文件等隐私，还会私自开启 / 关闭截屏、拍照、录音、wifi 等，造成用户隐私泄露，建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 任意代码执行漏洞（CVE-2018-15981）	该漏洞影响 Adobe Flash Player 31.0.0.148 及以前版本，成功利用会导致任意代码执行。该漏洞利用难度低且影响范围广，危害严重。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/Win32.GLDCT	此威胁是一种具有下载行为的木马类程序。该家族的样本会在执行后启动一个下载器来下载其他的恶意文件，并把自己添加到启动项中。在执行后会进行自删除，使自身难以被察觉。（威胁等级中）
		Virus/Win32.Renamer	此威胁是一种具有窃密回传行为的感染式病毒程序。该家族的样本在执行后会让攻击者获取计算机的完全控制权限，它可以窃取用户的信息并回传，并接受控制者发来的命令。（威胁等级中）
		Virus/Win32.ZAccess	此威胁是一种具有窃密回传行为的感染式病毒程序。该病毒家族的样本在执行后会在注册表中添加启动项，确保每次开机时启动。并且木马会连接两个服务器以接受命令并获取其他的恶意程序到本地。（威胁等级中）
		GrayWare[AdWare]/OSX.Bnodlero	此威胁是一种具有广告行为的灰色软件类程序。该病毒家族的样本仅在 OSX 平台上运行。该病毒家族的样本在安装后会产生广告弹窗。（威胁等级低）

2019 年企业面临的六大技术趋势

Calvin Hennick / 文　安天技术公益翻译组 / 译

在新的一年里，将会出现一些新技术，而一些已经出现的技术将会成为常态。

Ness Digital Engineering 公司首席技术官摩西·克兰克（Moshe Kranc）公布了他团队的研究成果：2019 年将改变“游戏规则”的六大总趋势以及特定的技术发展方向。他们预测：区块链和机器学习等较新的技术将进驻企业，云和大数据等相对熟悉的技术将继续巩固其地位，网络威胁将继续困扰企业。

下面，我们将讨论这些趋势，以及它们对企业 IT 管理人员的影响。

机器学习将会取得突破

“机器学习确实能落地。”克兰克说，“往往处于炒作周期中的很多技术尚未准备好迎接黄金时段，但是机器学习已经做好了准备，并且已经有了很多应用。我认为，我们仍然处于研究如何应用机器学习的早期阶段，其算法还有很大的改进空间。”

机器学习的一些应用，例如聊天机器人（chatbot），已经作为现成的解决方案提供。然而，克兰克表示，更复杂的用例——例如阅读放射图像或预测哪些客户最有可能流失的算法——要求企业寻找稀缺人才或与外部伙伴合作。

大数据越来越普遍

“如果你继续探索大数据平台，很可能会一路畅通。”克兰克说，“如果你认为大数据平台不稳定，很难找到合适的人才，而且好像没什么用，因而放弃大数据平台，那就大错特错了。”

克兰克解释说，大数据平台已经成熟，其市场逐渐缩小到少数更为稳定的解决方案上。与此同时，进入劳动力市场的年轻人正在将大数据知识带到他们的第一份工作岗位上。“他们从学校毕业，了解 Spark 和 Spark Streaming 的相关知识。”克兰克说，“现在，你已经能够找到这样的人才了。”（译者注：Spark 是一种开源软件，为分布式通用的计算集群框架，通过 API 接口，可支持 Windows、MacOS 和 Linux 等操作系统。Spark Streaming 是 Spark 的 API 编程扩展，支持扩容、高吞吐率以及容错率，特别适用于处理大容量实时数据流的业务场景。）

区块链的适度应用

克兰克说，经过一段时间的过度炒作，区块链将“回归现实”。

“我看到，区块链技术被用于很多不恰当的用例中。这只是因为，当它处于炒作周期的高峰时，使用它会显得很酷。”克兰克说。

克兰克说，对于分布式的、受控的、吞吐量要求不是太高的环境，区块链是最合适的。“假设你是沃尔玛，你所有的供应商都希望与你合作。”他说，“你可以要求他们使用你的区块链登记平台，来跟踪订购的货物、发出的货物以及订单是否已经付款等等。如果你能控制市场，那么区块链技术就是有用的。”

数字化转型不可避免

“你的竞争对手很可能已经完成了数字化转型，并且很可能正在从中获益。”克兰克说，“所以，如果你已经落后，你将不得不迎头赶上。这意味着创建一种透明的用户体验，让你的外部用户实时了解正在发生的事情，例如发货周期中的“产品到哪里了”。此外，数字化转型也发生在企业内部。例如，你订购了一些办公用品或培训项目，你的员工也希望能够跟踪它的位置。透明化（无论是内部还是外部）的趋势已经无法避免。如果你落后了，将会付出沉重的代价。”

网络安全仍然存在漏洞

“你必须认识到，安全是一场注定会失败的战争。”克兰克说，“相比于保护企业网络的安全人员来说，致力于攻破企业网络的黑客更多且更高明。此外，物联网将会使情况变得更糟糕，这是因为物联网系统在复杂性和安全保护方面倒退了一步。它们更加原始，因此更容易受到攻击。”

克兰克建议企业投资于外部渗透测试，以评估他们现有的安全措施。他说：“有太多公司认为网络安全在他们的掌控之下。安全措施是你自己设置的，你当然看不到它们的任何缺陷。你需要一双外在的眼睛盯着你的系统，让他们通过各种方法来攻击你的系统，以便了解系统存在哪些安全漏洞。”

云将成为常态——即使对于落后者也是如此

在公有云的早期阶段，出于对安全问题的担忧，许多机构对迁移到云犹豫不决。“随着越来越多的机构迁移到云，人们发现这些担忧不过是‘杞人忧天’。”克兰克说，“任何借口都无法阻止云迁移。”

克兰克表示，对于工作负载不是很沉重的机构来说，本地基础架构可能更加便宜。“但是，如果你正处于负载高峰期——比如说你正在研究机器学习，在机器学习的训练阶段，夸张点说，你需要使用全球所有的 CPU 10 秒钟。”他继续说道，“你可以购买所需的 CPU（其实这并不现实），然后让它们在一年中的其余时间闲置；或者你可以迁移到云端。这两种方法的成本可谓天差地别。”

原文名称	6 Tech Trends for the Enterprise in 2019
原文作者	Calvin Hennick，Calvin Hennick 是一位商业和技术作家。
原文信息	2018 年 11 月 16 日发布于 InformationWeek 原文地址 https://www.informationweek.com/big-data/6-tech-trends-for-the-enterprise-in-2019/d/d-id/1333277
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，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。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。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。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，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。

安天发布《AgentTesla 窃密木马样本分析报告》

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种名为 AgentTesla 窃密木马样本开始活跃。该恶意代码使用 .NET 语言开发，给样本的调试和分析带来了一定的困难，它可以自定义生成木马窃取信息，包括键盘记录、截屏、剪贴板记录以及摄像头图像等。

AgentTesla 窃密木马可以从电脑上提取还原多种登录信息缓存，包括浏览器中保存的网站账号密码，邮件客户端中保存的密码，FTP 工具、下载器中保存的密码等。它可以自定义木马将窃取到的信息回传给木马传播者的方式，包括网络接口方式、邮件方式以及 FTP 方式。在 FTP 方式下，工具使用者可以指定上传信息时用到的 FTP 地址、用户名和密码。在邮件方式下，工具使用者可以指定邮箱服务器地址、用户名和密码。如果使用者采用网络接口方式，则需要从工具官网下载一套完整的管理页面，并部署在自己的网站上。然后，使用者可以在工具中指定对应的网址作为 C&C 服务器，生成的木马运行后会连接该服务器并接收相应的指令，这些指令包括 uninstall、update、info、webcam、screenshots、keylog、passwords 等。

安天 CERT 提醒广大政企客户，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源是否可靠，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。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

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 BD 静态分析鉴定器、YARA 自定义鉴定器、文件来源信息分析鉴定器、数字证书鉴定器、文件元数据分析鉴定器、动态（Win7 x86）鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、动态行为鉴定器判定为木马程序。

概要信息

文件名	6ac38091a850ad01e2d1473ac67e0b161c25edc1aeba402b0f58659907a5164c
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	268 KB
MD5	C953507D30D40E41074B862A36F8E7B5
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Razy
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=C953507D30D40E41074B862A36F8E7B5

运行环境

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

危险行为

行为描述	危险等级	行为描述	危险等级
向其他进程内存写入数据	★★★	检测虚拟机	★★★★★
延时	★★★		

常见行为

行为描述	危险等级
打开自身进程文件	★
获取系统信息（处理器版本、处理器类型等）	★
获取驱动器类型	★
设置调试器权限	★
Run 自启动	★
创建特定窗体	★
壳行为填充导入表	★★
获取计算机名	★
启动指定服务	★
创建挂起进程	★★
.....	.....

进程监控

PID	创建	命令行
1372	target.exe	"c:\00f383610e1949218b0cf0007f0bfe27\share\target.exe"
192	target.exe	"c:\00f383610e1949218b0cf0007f0bfe27\share\target.exe"