安天周观察

主办：安天　2017 年 7 月 17 日（总第 95 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

赋能社会　共筑网安

安天承办“网安中国行 (2017)”黑龙江站系列活动

7 月 12 日，由国家互联网信息办公室指导，黑龙江省互联网信息办公室、中国网络空间安全协会主办，安天、哈尔滨工业大学等承办的“网安中国行——黑龙江站”系列活动在哈尔滨市友谊宫开幕。

“网安中国行”系列活动是中国网络空间安全协会 2017 年的重点工作之一，根据中央网信办的统一部署。7 月 12 日上午，“网安中国行 (2017)”——黑龙江站启动大会由黑龙江省互联网信息办公室副主任孙耀武主持召开，中国网络空间安全协会理事长方滨兴院士、黑龙江省互联网信息办公室主任李耀东、哈尔滨工业大学党委常务副书记熊四皓出席会议并致辞。来自中省直有关单位、社会组织、高校、科研院所和企业等单位的代表共计 400 余人参加了启动仪式。

安天首席技术架构师肖新光在启动仪式上发表了题为《能力型安全厂商在国家网络安全应急机制中的价值和使命》的演讲。

12 日下午，态势感知与有效防护主题高端论坛成功举办。中国网络空间安全协会理事长方滨兴等 6 位与会嘉宾分别作了发言，安天首席技术架构师就《可靠采集和有效防护对态势感知的支撑价值》发表演讲。

今年 2 月 17 日召开的国家安全工作座谈会上，习总书记强调“加强网络安全预警监测，确保大数据安全，实现全天候全方位感知和有效防护”，可以说，“有效”是对关键信息技术设施保障的基本要求。如果说态势感知能力是信息安全的顶层价值，那么有效防护就是其能力的基本盘。没有有效防护这个基本盘，威胁情报等各种能力手段，都将无法对接落地、形成价值。

因此，全天候、全方位的态势感知和有效防护是网络安全的核心需求。在此次活动展示区，安天响应网络安全发展趋势，特别对“可靠的数据采集、对关键基础设施的有效防护”的态势感知与监控预警平台进行了展示。

安天真功夫　亮相演武厅

在“网安中国行 (2017)”黑龙江站系列活动中，演武厅“技术创新秀”环节圆满落幕。安天在此环节现场展示了“基于资产可视化的基础设施攻防演练”、“安天智甲对未知病毒防护能力的演示”以及“扫地机器人攻击演示”，让现场观众近距离体验网络攻防，以此提升公众的网络安全防范意识。

基于资产可视化的基础设施攻防演练

对企业来说，资产是企业的核心，需要安全监控和威胁处置，用户关心自己的资产设备具体有哪些，是否采取了合理的防护手段。安天针对电力系统基础设施受到攻击的安全事件研发了攻防模拟演练场景，通过使用基于资产可视化分析技术的攻防场景展示组件来进行模拟事件并还原场景，以实现关键信息基础设施的仿真模拟与防护演练工作。

基于拓扑的资产可视化安全管控组件，是安天围绕自身提出的“交互式资产管理与威胁分析”这一理念而开发的可视化分析产品。它能够对资产在宏观、中观、微观多个维度上进行分析和呈现，使用户能够对其信息资产有全局性的管控，还能够对资产进行威胁分析、异常分析，并快速定位威胁、做出处置，保护信息资产的安全。

安天智甲对未知病毒防护能力的演示

在 5 月 12 日晚全球爆发勒索蠕虫“魔窟”(WannaCry) 事件后，用户对网络空间安全更加重视。此次“技术创新秀”上，安天工程师介绍并演示了在没有防护的情况下 WannaCry 病毒的攻击效果，使用 2016 年版本的安天智甲对 WannaCry 病毒进行有效防护，体现了安天智甲的未知病毒防护能力。

扫地机器人风险演示

扫地机器人作为一款智能家居设备，随时会接入家庭的 WiFi 网络，如果家用 WiFi 密码配置被破解，攻击者能够对扫地机器人做什么？安天工程师在现场演示了使用 PC 获取扫地机器人的控制权，从而控制扫地机器人的运动方向，并获取到扫地机器人内置摄像头回传的摄像数据的过程，造成安全隐患。以此提醒广大用户提高安全意识，及时做好安全风险防范。

同时，安天提示个人和家庭用户提高安全意识和安全习惯，对于电脑、手机、IoT 设备等应按照安全要求及时进行维护、更新、升级，保持我们常用的安全产品随时得到安全维护，保证我们的 PC 机、家用 WiFi 设置高强度的安全密码等，以降低产品的安全风险。

每周安全事件

类 型	内 容
中文标题	印度发生最大规模数据泄漏事件，超过 1 亿用户信息被曝
英文标题	India's largest data leak occurred more than 100 million user information was exposed
作者及单位	Promit Mukherjee；Reuters
内容概述	近日，据外媒报道，印度电信运营商 Reliance Jio 的一亿多用户数据被泄漏到 Magicapk.com 网站上，包括姓名、手机号、电子信箱、SIM 激活日期，甚至还包括 Aadhaar 号码（身份识别信息）。 业内人士认为，如果消息属实，这可能是印度电信史上最大规模的用户数据泄漏事件。目前，Reliance Jio 正在调查此事，但已初步表示，Magicapk.com 网站上发布的数据似乎并不真实。但是，已经有许多 Reliance Jio 用户在 Twitter 上抱怨，称自己个人资料被曝光。此外，一些印度媒体经过调查后证实，Magicapk.com 上的数据是真实的。对此，Reliance Jio 发言人称：“针对数据泄露一事，我们已经通知了执法部门，将来我们还会继续跟进。”
链接地址	https://www.reuters.com/article/us-reliance-jio-cyber-idUSKBN19U10X

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 个移动平台恶意代码和 4 个 PC 平台的恶意代码值得关注

平台分类	关注方面	名称	相关描述
移动恶意代码	较为活跃样本	Trojan/Android.Hqwar.f [prv，exp，rmt]	该应用程序运行后会诱导激活设备管理器，访问钓鱼网页，窃取用户银行账户相关信息，接受远程指令，进行发送短信、下载应用，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.fakewechat.j [exp]	该应用程序伪装成微信应用，运行后静默下载安装未知应用，并将其写入系统应用，造成用户资费损耗，影响系统安全，建议不要安装。（威胁等级高）
		Trojan/Android.nbank.c[prv]	该应用程序包含风险代码，窃取用户通讯录、收件箱和通话记录等隐私信息上传，造成用户隐私泄露。（威胁等级高）
		Tool/Android.SMSBomber.aq[exp]	该应用程序运行后，会输入短信号码及内容后自动发送短信。用于短信轰炸，同时也会产生资费消耗。（威胁等级中）
		Trojan/Android.emial.ga[prv，exp]	该应用程序运行后隐藏图标，获取用户短信和通讯录并联网上传，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.Triada.aw [exp，rog]	该应用程序运行会动态加载恶意子包，私自下载安装恶意应用，警惕该程序造成用户资费损耗和隐私泄露。（威胁等级高）
		Trojan/Android.PinkApp.b [exp]	该应用程序包含风险代码，运行会隐藏图标，关闭 Wi-Fi，加载广告推广应用，造成用户流量资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.LockerMaker.b [spr，exp]	该应用程序为锁机生成器工具，运行后诱导用户购买激活码等手段注册来使用，恶意传播、制造勒索应用，建议卸载。（威胁等级高）
		G-Ware/Android.LockScreen.ai[rog，lck]	该应用程序伪装成抢红包应用，运行后锁定屏幕，会造成用户资费损失、手机无法正常使用，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	Apache Struts2 远程代码执行漏洞 S2-048 CVE-2017-9791	Apache Struts 发布最新的安全公告，漏洞编号为 S2-048(CVE-2017-9791)，该漏洞存在 Struts2 和 Struts1 一个 Showcase 插件 Action Message 类中，通过构建不可信的输入实现远程命令攻击，存在安全风险。（威胁等级高）
	较为活跃的样本	Trojan[DDoS]/Linux.Ddostf	此威胁是一类针对 Linux 平台的具有 DDoS 功能的木马家族。该家族样本运行后连接远程服务器，向其发送系统敏感信息。它可以接收远程服务器的命令并执行 DDoS 攻击，包括 TCP、UDP 及 HTTP 的洪水攻击。（威胁等级中）
		Trojan[Ransom]/Win32.Radam	此威胁是一类可以加密用户文件并勒索赎金的木马家族。该家族样本运行会加密用户文档并要求付费，只有按时付费才可以解密，有一定威胁。（威胁等级高）
		Trojan[Ransom]/Win32.Cryptor	此威胁是一类可以加密用户文件并勒索赎金的木马家族。该家族样本运行后遍历系统磁盘并加密文件，向用户勒索赎金以解密，有一定威胁。（威胁等级低）
		Trojan[Banker]/Win32.Banaris	此威胁是一类以窃取网络银行敏感信息为目的的木马类程序。该病毒伪装成正常数据，以获取认证。该病毒利用各种途径，使黑客获得数字证书来伪造文件。该家族会收集用户的机密信息，如网上银行详细信息和密码等，并将窃取的数据发送给远程黑客。（威胁等级高）

IP 盗窃和网络敲诈风险日益严重

Robert McFarlane / 文　安天公益翻译小组 / 译

最新的《Verizon 数据泄露事件报告》警告说，旨在窃取知识产权 (IP) 和公司机密的网络间谍攻击正在兴起，这些风险都是由廉价的黑客工具和加密货币驱动的。

娱乐巨头迪士尼被黑客入侵，黑客盗走了未上映的《加勒比海盗 5：死无对证》，要求迪士尼支付赎金，否则就公开影片。迪士尼拒绝了。

在迪士尼攻击事件之前，一名黑客窃取了 Netflix 尚未播出的《女子监狱》第五季全集， Netflix 拒绝支付赎金，该剧便在网上遭全集泄露。

公司应该担心 IP 盗窃

Verizon 的报告指出，网络间谍活动尤为关注制造业 (占 90%)。大多数此类网络间谍活动是由国家威胁源发动的，旨在窃取尖端技术供本国使用。

然而，迪士尼攻击事件显示，不开发耐虫超级作物或基因治疗的公司也会被当成攻击目标。有些企业对网络敲诈的概念嗤之以鼻，认为他们无关紧要，不足以吸引黑客的注意。但是，正如 Verizon 的报告所述，行业和规模并不重要，“如果您有 (或者黑客认为您有) 有用的信息，就会成为 IP 盗窃的潜在目标。”

如今，这一标准几乎适用于所有人，攻击者的目标包括：专有金融技术解决方案，赌场游戏软件，秘密食谱，移动应用程序，甚至公司秘密 (如营销策略、员工招聘或新产品研究的资料)。当然，没有发行的书籍、电影、电视剧等都是目标。

此外，黑客不再需要雄厚的资金和高明的技术，就能够入侵企业系统。

加密货币和“傻瓜恶意软件”降低了黑客门槛

以前，计算机黑客攻击需要高超的技术实力。然而，暗网 (Darknet) 的迅速发展使得他们可以购买廉价，易于使用的基于云的“傻瓜恶意软件”。有一群力争进取的黑客甚至提供客户支持，帮助客户解决遇到的问题。

比特币等加密货币的崛起也有助于网络勒索的增长。任何人都可以注册一个比特币账户，随心所欲地发送、接收和花费资金，无需担心暴露自己的身份和住址。

第三方供应商可能使大企业面临风险

Netflix 攻击事件揭示了另一个 IP 安全问题：大公司的安全水平受到第三方业务伙伴的影响。

现在，大量易于使用的工具和不可追踪的支付方式，以及公司 (包括许多第三方供应商) 在网络上存储着价值数百万美元的知识产权的事实，促使网络犯罪分子越来越有创意。入侵者不必渗透 Netflix 本身，而是劫持了 Netflix 的第三方后期制作厂商 Larson Studios。同样，犯罪分子可能会入侵服装品牌的纺织品供应商，窃取下个季度的所有款式设计；或者入侵真人秀选手的手机，在大结局播出前公布获胜者。

在某些情况下，入侵一个小供应商可能比攻击跨国公司更有利可图。

对抗 IP 盗窃

网络保险公司已经注意到第三方供应商漏洞问题了；一些政策要求组织确保其业务伙伴的系统安全。但是说起来容易做起来难。虽然像迪士尼这样的大型公司能够在其系统上实施诺克斯堡级别的安全措施，但这些措施可能会破坏小企业的预算。不过，迪士尼和 Netflix 表示，只有庞大的预算并不能保证安全。

一个客户端解决方案是网络分段：公司为供应商创建一个独立的系统，使用独立的设置来处理任务，尽可能减少与公司主系统的连接和数字足迹。然而，这涉及成本问题，在某些情况下 (如 Netflix 案例)，供应商可能需要高度专业的软件和硬件来完成其工作，这使得创建这样一个孤立的系统不太可能。

另一个成本较低的解决方案是：供应商完全在云中工作，与大公司的系统隔离。供应商不能将数据下载到自己的网络上，云解决方案应使用双因素身份验证 (密钥卡或应用程序) 进行安全保护，以避免与登录凭证有关的安全问题。这种设置并不是万无一失的，而且可能要求供应商投资实现更快速的连接或处理较慢的速度，但是能够减轻其经济负担。

最后，各种规模的组织应考虑与托管安全服务提供商 (MSSP) 合作。使用 MSSP 比内部执行网络安全功能更加便宜，特别是组织不必在安全人员、软件和硬件方面投资了。

随着知识产权的存储数字化，IP 盗窃和网络勒索可能会成为像勒索软件一样严重的问题。各种规模的企业必须摆脱这种威胁，了解风险，采取积极措施防范风险。

原文名称	The Growing Danger of IP Theft and Cyber Extortion
作者简介	Robert McFarlane(罗伯特·麦克法兰)，托管安全服务提供商 (MMSP) 和咨询公司 Mosaic451 的首席营收官，拥有 20 多年的电信、数据网络和网络安全业务开发经验。
原文信息	2017 年 6 月 27 日发布于 Dark Reading 原文地址 http://www.darkreading.com/cloud/the-growing-danger-of-ip-theft-and-cyber-extortion/a/d-id/1329247?
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《Staser 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注意到，一种可以对抗安全软件且通过移动设备与 IPC$ 传播的恶意代码家族在网络上比较活跃，该家族名为“Staser”。

该家族样本运行后，首先会打开与当前病毒进程文件同名的信号互斥量，并判断互斥量是否存在，若存在即不会继续运行。其次，恶意代码通过注册表查找判断瑞星杀毒软件的存在，创建进程快照；判断 360 的杀毒软件进程 360sd.exe、360rp.exe 是否存在，如果存在，则结束它们的运行。它还会在用户桌面右下角伪造 360 的弹窗界面迷惑用户。

恶意代码可以利用 IPC$ 入侵用户主机，利用弱口令猜测用户主机的帐号密码，成功后复制自身到计算机系统目录中执行。另一种传播方式则通过移动设备传播，恶意代码会在连接主机的移动设备中释放病毒文件 autorun.inf，复制自身到移动设备中，设置文件属性为系统、隐藏。导致用户在插入移动设备到主机时，恶意代码即感染主机。

此外，恶意代码样本还会创建服务，将自身复制到 %system% 目录下，文件名为 6 个随机字符。恶意代码创建线程，连接远程服务器，收集系统的版本、CPU、内存等信息并回传，接收远程命令进行恶意操作，如 DDoS、下载文件到指定目录、创建进程等。

安天提醒广大网络用户，不要随意点击或复制邮件中的网址，不要轻易下载来源不明的附件。对于移动设备一定要安全使用，在公共场合的计算机中不要插入自己的工作移动设备，以防感染工作主机及家用机，导致恶意代码广泛传播。

目前，安天追影产品已经实现了对该类样本的检出。

木马程序

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

文件被页面手工提交发现，经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、数字证书鉴定器、可交换信息 (EXIF) 鉴定器、动态行为 (Windows7) 鉴定器、静态分析鉴定器、动态行为（默认环境）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、静态分析鉴定器、安全云鉴定器将文件判定为木马程序。

根据动态行为 (Windows7) 得出该文件具有以下行为：在注册表中查找反病毒软件、使用 cmd 删除自身、删除自身、遍历进程、释放 PE 文件、复制文件到系统目录、创建服务、启动服务、查找指定内核模块、创建特定窗体、获取驱动器类型、访问 dns、结束进程、自启动。

根据动态行为（默认环境）得出该文件具有以下行为：在注册表中查找反病毒软件、使用 cmd 删除自身、删除自身、其他进程写入可疑数据、延时、查找指定内核模块、遍历进程、结束进程、打开自身进程文件、释放 PE 文件、复制文件到系统目录、创建服务、获取驱动器类型、启动服务、创建特定窗体、获取计算机名称、请求加载驱动的权限、获取主机用户名称、访问 dns、连接网络、获取 CPU 信息、填充导入表（疑似壳）、获取系统内存、独占打开文件、自启动。

文件名	803C617E665FF7E0318386E24DF63038
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	61 KB
MD5	803C617E665FF7E0318386E24DF63038
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Staser
判定依据	安全云

运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office 2007、flash、wps、FoxitReader、adobe reader

报告地址：https://antiy.pta.center/_lk/details.html?hash=803C617E665FF7E0318386E24DF63038

危险行为

行为描述	危险等级	行为描述	危险等级
在注册表中查找反病毒软件	★★★	删除自身	★★★★
使用 cmd 删除自身	★★★★		

其他行为

行为描述	危险等级	行为描述	危险等级
遍历进程	★	释放 PE 文件	★
复制文件到系统目录	★★	创建服务	★
启动服务	★	查找指定内核模块	★
创建特定窗体	★	获取驱动器类型	★
访问 dns	★	自启动	★
结束进程	★		