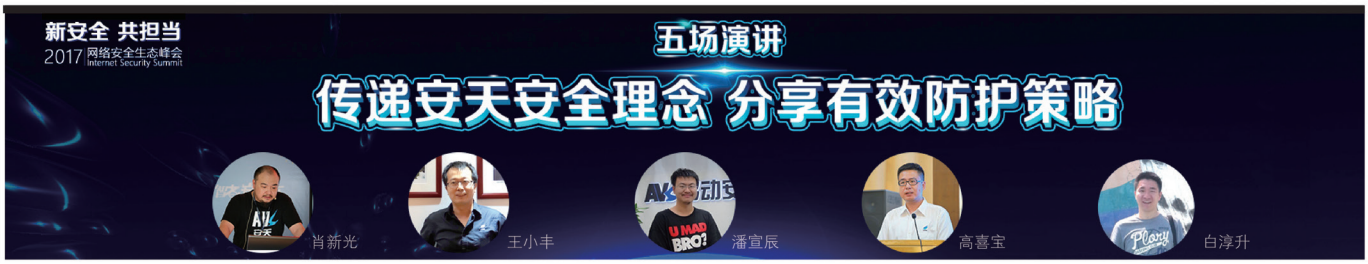
安天周观察

主办：安天　2017 年 7 月 31 日（总第 97 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流



五位安天人亮相 2017ISS 峰会并发表演讲

7 月 26-27 日，以“新安全，共担当”为主题的 2017 网络安全生态峰会 (2017 Internet Security Summit，ISS) 在北京国家会议中心举行。五位安天人出席峰会并发表演讲，五场演讲合力传递出安天安全理念，分享了有效防护策略，展现了安天防御能力。

主会场：安天首席架构师肖新光

态势感知的支撑和价值落地

真正的态势感知应走向“鹰的眼睛、狼的耳朵（复合感知）、熊的力量（支撑体系）、豹的速度（响应）、人的大脑（决策）”这样一个可有效进行观察、思考、决策的体系，而非变成一只“孔雀”，其整体价值都被表现力所干扰。肖新光提出，对于态势感知而言，应该有“感”才有“知”，而当前“感”的能力还不足够，未能实现有效支撑价值，因此需要改善我们的采集和对象处理。

最后他强调，态势感知不只是一种防御侧能力，强大的攻击方也一直在建立相应的态势感知能力。需要警惕的是，我们在万花筒里自以为看尽了世界，而对手却在阴影里用望远镜详细看着我们。不遗余力地去感知真实态势，做好真态势感知是安天人共同的理想。

圆桌对话：安天研发副总裁王小丰

网络安全与公众生活

王小丰简要阐述了 WannaCry 事件的反思。他表示：本次事件恰恰是把基于高级漏洞攻击的穿透性和勒索的高感知度结合在一起，结果产生了较大的社会影响，也验证了我们防御体系长期投入的不足。过于依赖网络边界的隔离防护而忽视内部节点的配置加固、补丁升级和安全软件的及时更新等现状急需改变。有效的端点安全防护系统，必须立足于操作系统不可能完美升级的假设下，建立有效的应对威胁的防护能力需要用户和安全厂商共同努力。

企业基础安全与应急响应分论坛：安天安全专家高喜宝

魔窟的水面之上和水面之下

高喜宝从 WannaCry 病毒谈起，着重讲述了网络病毒在网络战争中的常用手段和作用。如今的信息系统不再是简单的 IT 应用场景，更需要形成全方位的态势感知能力。越是高级的攻击越会形成一种武器组合链条，越是衔接越会使高级成为某种弱点。如何对攻击链实现有效的遏制、呈现并最终阻断于核心资产之前，是我们在关键基础设施防御中的一个重要方法。他强调，今天任何一个单一的环节都不足以应对网络攻击，必须通过有效的信息采集、数据处理和深度挖掘，形成上层的态势感知、安全监测和通报预警等安全能力，才可能构成最终的安全价值。

移动安全分论坛：安天移动安全公司 CEO 潘宣辰

移动威胁对抗的人机协作和思辨

潘宣辰结合移动威胁在过去 5 年里不断升级和迁移的变化，与观众分享了移动威胁对抗的过程和特点，对移动威胁的模型和所呈现出的长尾分布规律下移动威胁分布的特点、针对性的技术对抗策略等作了技术分享。

随后，他从机器学习的视角对基于人机协作体系的威胁对抗工程化体系的基础架构的设计规划进行了阐述。安天期望能够在高精度的检测和分类基础上，以业务价值结合情报驱动的策略来帮助客户务实有效的防御威胁和落地安全价值。他希望安天的核心能力可以成为一种纽带，将安天的能力体系和客户的安全体系聚合起来，建立起一个纵深防御体系，构建出更好的综合防御能力。

威胁情报与安全智能分论坛：安天恶意代码分析工程师白淳升

基于威胁情报的攻击组织画像与溯源

白淳升从白象、魔窟两起真实攻击案例的溯源过程引入，阐述了两起事件的溯源过程，并对网络攻击溯源的一些具体方法和技术手段进行分享，进而探讨了如何将这种方法和一些必要的数据纳入到威胁情报体系，使当前的威胁情报可以更好的对网络攻击组织进行画像和溯源，最后基于当前攻击者反溯源和构建虚假情报的案例，指出了威胁情报溯源面临的干扰和可信性问题。

每周安全事件

类 型	内 容
中文标题	著名的 Android 勒索程序 SLocker 源码在网上泄露
英文标题	SLocker decompiled code leaked online for free，a gift for crooks and hackers
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，Android 平台最流行的勒索程序家族之一，SLocker 恶意程序源码在网上泄露，攻击者可因此开发变种。 GitHub 一个名为“fs0c1ety”的用户公布了源码，这名攻击者还邀请所有人共同来完善代码。SLocker 最早是在 2015 年被发现的，这是第一款能够加密 Android 文件的勒索程序，文件类型包括图像、文档、视频等。这款恶意程序假装执法机构，让受害者支付赎金。SLocker 去年感染了数千款 Android 设备，今年 5 月市面上涌现的 SLocker 变种就已经超过 400 种。此外 SLocker 还能劫持设备，让用户无法使用设备。在其源码公布后，未来几周内，预计 SLocker 变种将变得更多。
链接地址	http://securityaffairs.co/wordpress/61323/malware/slocker-source-code.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 个移动平台恶意代码和 5 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	新出现的样本家族	RiskWare/Android.qxsc.a[exp] 2017-07-25	该应用程序运行后会诱导用户分享和下载安装推广应用，会造成用户资费消耗。（威胁等级低）
		Trojan/Android.SmsGame.a[exp] 2017-07-25	该应用程序多为游戏应用，包含风险行为代码，运行会私自发送短信、拦截短信，会给用户造成资费消耗，建议不要使用。（威胁等级高）
		Tool/Android.SmsLocation.a[exp，prv] 2017-07-27	该应用程序运行获取用户地理位置，短信发送给用户设定的手机号，会造成用户隐私泄露和资费消耗，建议谨慎使用。（威胁等级中）
	较为活跃样本	Trojan/Android.SmsThief.bh[prv，exp]	该应用程序运行无实际功能，运行后上传用户收件箱内容，后台拦截并上传短信，造成用户隐私泄露和资费损耗。（威胁等级中）
		Trojan/Android.b4aspy.g[prv，spy]	该应用程序伪装成安全软件，运行后激活设备管理器，窃取短信、照片、联系人等信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.henbox.b[prv，rmt，exp]	该应用程序伪装成备份应用，运行后隐藏图标，后台获取远程指令，窃取用户手机基本信息、短信、联系人、地理位置、网络信息、QQ 及微信的联系人等隐私，私自进行录音、拍照，并上传，加载提取文件，造成用户隐私泄露和流量消耗。（威胁等级高）
		Trojan/Android.SmsSend.mr[exp，fra]	该应用程序运行后申请短信发送权限，静默发送短信，会造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.QQspy.cl[prv]	该应用程序运行后要求用户填写 QQ 和手机号码并上传，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 内存破坏漏洞 (CVE-2017-2930)	Adobe Flash Player 是美国 Adobe 公司开发的一款被广泛使用的、专有的多媒体程序播放器。Adobe Flash Player 中存在内存破坏漏洞，攻击者可利用漏洞控制受影响的系统，导致任意代码执行。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Delf	此威胁是使用 delphi 语言编写具有下载行为的木马类程序，运行后会连接网络并下载其它恶意程序执行。通过以邮件、挂马、捆绑正常软件来进行传播。（威胁等级中）
		Trojan[Downloader]/JS.JScript	此威胁是一种具有下载行为的木马类程序。脚本运行后会执行里面的代码，链接网络下载恶意文件。通常以网页挂马和邮件进行传播。（威胁等级中）
		Trojan[Downloader]/Win32.VB	此威胁是一种以 VB 语言开发的，具有下载功能的木马类程序。该家族样本会在系统启动时自动运行。通常是从网页中下载或是捆绑正常程序。这种类型的恶意代码通常会在用户访问具有漏洞的网站时感染计算机。（威胁等级中）
		Trojan[Backdoor]/Linux.Gafgyt	此威胁是一种木马类后门程序，运行在 linux 平台，主要功能为 DDoS 攻击、更新和下载等。通过扫描 SSH 弱口令进行传播。（威胁等级中）

物联网安全事件日益猖獗且成本高昂

Dawn Kawamoto / 文　安天公益翻译小组 / 译

近日，两份独立的研究报告均显示，物联网设备攻击导致 46% 的受访者遭受了攻击事件。

IDC 本月发布的一项调查采访了大约 100 名 IT 安全人员、IT 运营人员和高管。而另外一项调查是由咨询公司 Altman Vilandrie & Co. 在今年 6 月份发布的，他们采访了 19 个国家的大约 400 名 IT 高管。

根据 Altman Vilandrie 的报告，在未来的几年内，保护 IoT 设备的成本将会增加，甚至高达 IT 预算的三分之一。绝大多数 IDC 受访者表示，处理物联网攻击的成本往往超过传统攻击。

IoT 安全和公司规模

根据 Altman Vilandrie 的报告，在年收入低于 4.99 亿美元的公司中，物联网攻击导致超过一半的公司面临高达 25 万美元的经济损失。同时，调查显示，九家年收入超过 50 亿美元的公司的损失至少达到 2000 万美元。Altman Vilandrie 负责人兼报告作者之一的瑞恩・迪恩 (Ryan Dean) 表示：“在我们的研究样本中，年收入超过 50 亿美元的公司只有 5%。总的来说，最大规模的企业遭受的经济损失可能会有很大的不同，这取决于攻击类型和影响。”

IoT 攻击成本 vs 传统攻击成本

IDC 报告显示，46% 的调查对象遭遇了物联网设备攻击。同时，63.5% 的金融服务行业受访者和 47.2% 的医疗行业受访者表示，他们的组织经历了物联网安全事件。报告发现 70.1% 的受访者表示与传统攻击相比，物联网攻击的成本更高。

两年内 IoT 安全情况

在两年的调查时间里，46% 的 Altman 受访者表示其物联网设备或网络遭遇了攻击。

迪恩表示，首席信息安全官 (CISO) 应该意识到三大物联网安全隐患。首先是缺乏物联网安全投资，这可能会导致物联网攻击。其次是没有意识到物联网攻击不仅会损坏设备及其周围环境，而且还会导致经济损失、品牌声誉损失和其他损失。第三是，如果 CISO 不愿意将成熟安全厂商与 IoT 安全创业公司进行权衡比较，那么他们可能会面临风险。

投资回报率

调查结果显示，将物联网安全纳入 IT 安全预算的公司更不容易遭遇物联网攻击。迪恩说：“IoT 安全投资较少的公司，在本案例中是 20% 的 IT 预算，更容易遭受 IoT 攻击。相反，对 IoT 安全投资更多的公司，在本案例中是 33% 的 IT 预算，更不容易遭到攻击。”

IoT 安全支出

IDC 发现，物联网市场虽然年轻，却在快速成熟，40% 的受访者表示，他们的公司已经实施了六到十项物联网安全措施。金融服务和医疗机构预测，物联网安全成本将会增加。

IDC 的韦斯特维尔特表示，目前 IoT 安全占 IT 预算的 15% 或更少。他指出，随着公司添加端点、网络和 Web 安全解决方案，他们将需要扩展到物联网环境中。

金融与医疗行业 IoT 支出增加

IDC 调查发现，62% 的受访者预计 IT 安全支出将会增加。金融服务和医疗机构预测，他们将会采取安全分析、数据丢失预防和其他传统 IT 解决方案来减轻物联网风险。

韦斯特维尔特说：“IoT 医疗设备使用传感器进行通信，医疗行业的很多 IoT 安全支出源于需要遵循合规性。”

购买 IoT 安全解决方案的主要原因

根据 Altman Vilandrie 的报告，失去对 IoT 设备的控制是 IT 高管购买 IoT 安全解决方案的主要原因之一。迪恩说，这是由公共安全问题驱动的，例如吉普切诺基的远程控制。

排名第一的是 No. 1 原因 (保护客户信息) 和 No. 2 原因 (失去对 IoT 设备的控制) 的组合。在解释为何将这两个原因进行组合时，迪恩表示这样做是为了广泛地反映 IT 高管需要关注的重要问题。

IoT 安全解决方案购买清单

调查发现，在遭受了物联网攻击的企业中，71% 将“防御技术”列为他们在未来几年内最想要购买的解决方案。对于尚未遭受物联网攻击的公司而言，最想要购买的 IoT 安全解决方案是监控和控制产品。

“我们认为，购买‘防御产品’是一种应对型措施，”迪恩表示，“这些受访者已经遭遇了物联网攻击，尚未部署足够的安全防御解决方案。相反地，其他受访者可能已经部署了良好的安全方案，他们更加注重购买‘监控和控制产品’来管理端点和系统。”

原文名称	IoT Security Incidents Rampant and Costly
作者简介	Dawn Kawamoto，Dark Reading 副主编，主要关注网络安全新闻和趋势。
原文信息	2017 年 7 月 18 日发布于 Dark Reading 原文地址 https://www.darkreading.com/vulnerabilities---threats/iot-security-incidents-rampant-and-costly/d/d-id/1329367

安天发布《Adwind RAT 恶意代码家族分析报告》

近日，安天 CERT(安全研究与应急处理中心) 分析人员发现，一种可以跨平台的远程访问木马 Adwind RAT，采用 Java 编写，能感染几乎所有的主流操作系统，包括 Windows、Mac OS、Linux 和 Android。该恶意家族一般通过垃圾邮件传播，主要针对航空工业领域的企业，受严重影响的国家地区有瑞士、乌克兰、澳大利亚和美国等。

从 2017 年 1 月开始，Adwind 活跃程度不断增加，在 2017 年 5 月到 6 月之间，Adwind 的出现频率增长了 70%，这也表明攻击者正积极地推送和传播 Adwind。Adwind RAT 具有窃取用户证书、收集和记录键盘信息、截屏以及从目标系统窃取数据等恶意行为。攻击者曾利用 Adwind 的变种版本攻击银行等企业，Adwind 甚至还可以用受感染设备组成僵尸网络。

Adwind 主要通过垃圾邮件传播，在 2017 年 6 月，Adwind 使用了不同的 URL 地址来向目标用户传播由 .NET 编写的恶意软件，而且这些恶意软件还具备间谍软件的功能。另一次感染则是使用了不同的域名托管恶意代码与 C2 服务器。两次均使用了社工的方法，使用户点击恶意 URL 地址。该恶意 URL 会投放一个程序信息文件 (PIF)，其中包含关于 Windows 如何运行 MS-DOS 应用的信息，并且可以像可执行程序一样直接运行。这个文件采用 .NET 编写，其功能相当于一个下载器。下载器会通过调用 Windows API 来尝试修改系统证书，系统证书被恶意篡改之后，下载器便会从一个域名下载 Payload、动态链接库 DLL 和 7-Zip 安装程序，而这个域名指向的是垃圾邮件操作者所使用的文件托管服务器，域名为 https://nup.pw。

安天建议广大用户在使用 Java 工作时应该注意安全，及时更新 Java 版本。对于社会工程学技术也应当有所防备，在收到垃圾邮件时不要随意点击其中的 URL 及打开附件。目前，安天追影威胁鉴定器已经实现了对 Adwind 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：

文件被内部组件、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、可交换信息 (EXIF) 鉴定器、数字证书鉴定器、动态行为 (Win7) 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 BD 静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

文件名	51f9e895441dffdf8e47c83208f85993
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	7 KB
MD5	51F9E895441DFFDF8E47C83208F85993
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Skeeyah.A!rfn
判定依据	BD 静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=51F9E895441DFFDF8E47C83208F85993

运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office2007、flash、wps、FoxitReader、adobe reader

其他行为

行为描述	危险等级
打开自身进程文件	★★

根据动态行为 (Win7) 得出该文件具有以下行为：打开自身进程文件。

根据动态行为 (默认环境) 得出该文件具有以下行为：延时、获取系统内存、打开自身进程文件、获取计算机名称、查找指定内核模块、创建特定窗体、获取系统版本、获取主机用户名称、获取驱动器类型、启动服务、访问 dns、独占打开文件、查找浏览器进程、查找特定窗体、获取 socket 本地名称。

运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认、ie6、office2003、flash、wps、foxit reader、adobe reader

危险行为

行为描述	危险等级
延时	★★★

其他行为

行为描述	危险等级	行为描述	危险等级
获取系统内存	★★	打开自身进程文件	★
获取计算机名称	★	查找指定内核模块	★
创建特定窗体	★	获取系统版本	★★
获取驱动器类型	★	获取主机用户名称	★
访问 dns	★	启动服务	★
查找浏览器进程	★★	独占打开文件	★
获取 socket 本地名称	★	查找特定窗体	★