安天周观察

主办：安天　2017 年 3 月 13 日（总第 79 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布 2016 年安天移动安全年报

3 月 10 日，安天移动安全团队在官方博客上发布《2016 年安天移动安全年报：威胁的全面迁徙》（以下简称年报），对 2016 年网络威胁状况进行总结，对威胁演进趋势做出预测。

安天从 2005 年开始，每年年初公布年报，并分成“基础威胁年报”和“移动安全年报”发布。

安天移动安全团队 2016 年度报告以“威胁的全面迁徙”为主题，以观点的方式来组织内容，用威胁的概念表达归纳安全事态的现象和趋势，并新增“反思”和“应对”两个版块，探寻观点和现象背后的原因，提出应对建议。安天移动安全团队希望通过这份年度报告，向移动安全行业从业者、移动互联网相关企业以及大众用户分享和传达我们的所见、所为及所思。

2016 年的移动威胁呈现出了一些新特点：伴随移动的快速发展，企业和组织逐渐引入移动办公和移动政务，终端数据的商业价值日益凸显，移动威胁正在从个人向企业组织迁移；针对移动终端的 APT 攻击也将随之高发；伴随移动云服务等新兴技术模式的兴起，业务欺诈类的安全问题也开始成为移动安全的关注点；从技术演进上看，Root 型恶意代码、勒索软件、色情应用等也在进行快速的技术演进，给技术对抗带来了新的挑战；Android 系统需扮演攻防的主要战场，同时 iOS、嵌入式 Linux 以及各种 IoT 设备也出现新的威胁趋势和特点，增加了移动威胁全局对抗的深度和战线的广度。

本年度的安天“基础威胁年报”承载了更多相对系统而沉重的思考，历经了多个版本的修改，将于稍后发布。安天移动威胁年报可在安天移动安全官方博客或安天微信公众号查看。（完整报告：http://blog.avlsec.com/2017/03/4474/2016-security-report/）

安天为广西电网提供恶意代码安全防护解决方案

电力行业是国民经济的基础产业，是关键基础设施之一，同时也是网络攻击的重要目标。

广西电网作为国有特大型企业，负责为广西经济社会发展提供电力保障，承担着投资、建设和经营输配电业务。近些年来，电力信息化建设取得了非常显着的成就，信息化建设已经有了一定的规模，然而电力行业的信息系统庞大而又复杂，IT 系统治理难度非常之大，这给广西电网企业管理人员带来了不小的压力。

广西电网为保证生产、调度、管理等环节的网络安全，需要为生产控制大区和管理信息大区的终端部署终端反恶意代码系统，并且要求：运行各类操作系统的终端可统一管理；能够实现多区终端统一管理，各省、地市分级管理；针对移动存储介质实现细粒度统一管控。

安天安全服务团队针对广西电网的终端管理防护需求，提供了由智甲终端防御系统以及移动介质统一管理系统组成的恶意代码防护安全解决方案。该方案完美实现了用户终端管理防护需求，而且智甲终端防御系统对 Windows、Linux、国产（中标麒麟、中科方德、银河麒麟）、Unix 等操作系统实现了良好兼容。

安天提供的恶意代码安全防护解决方案，旨在提升广西电力调度中心终端整体安全性和管理效率，实现了对移动介质认证注册、授权管理、行为审计、加密管理、使用管理等细粒度管控。智甲终端防御系统可在病毒特征库不升级的情况下，仍可通过策略等安全机制进行安全管控，持续保证用户终端安全。

安天获『国家网络与信息安全信息通报机制先进技术支持单位』

日前，由公安部第十一局、国家网络与信息安全信息通报中心主办的“国家网络与信息安全信息通报机制技术支持 2016 年度工作总结会议”在京召开。

公安部网络安全保卫局总工程师郭启全、国家网络与信息安全信息通报中心十处处长黄小苏、公安部第一研究所副所长冯曰铭出席了本次会议。安天被授予“2016 年度国家网络与信息安全信息通报机制先进技术支持单位”证书。

此次，是安天连续第三次获得“国家网络与信息安全信息通报机制先进技术支持单位”，是主管单位对安天信息通报工作的充分认可。

安天凭借 17 年的技术积累，在反病毒引擎、海量恶意代码分析体系、高级持续威胁分析等方面的分析和检测能力，多次在国家重大网络事故和网络安全事件的应急响应中发挥了关键作用，参加了包括北京奥运会、上海世博会、2010 年起历届两会、2014APEC 会议、抗战胜利 70 周年阅兵、G20 峰会等重大活动的网络安保工作，并荣获重大活动信息安全保卫工作突出贡献奖，多次受到各级有关部门的通令嘉奖。

未来，安天将继续充分发挥自身的优势，持续为网络与信息安全的信息通报工作贡献力量，为网络安全的态势感知和通报预警工作提供支持。

每周安全事件

类 型	内 容
中文标题	100 万被解密的 Gmail 和雅虎账户在暗网出售
英文标题	Hacker Selling Over 1 Million Decrypted Gmail and Yahoo Passwords On Dark Web
作者及单位	Swati Khandelwal；The Hacker News
内容概述	近日，昵称“SunTzu583”的供货商在暗网市场出售数百万 Gmail 和雅虎账户。账户清单于本周挂出，显示所售账户为从 2012 年 Last.FM 数据泄露获取到的 10 万个雅虎账户——Last.FM 数据泄露事件中 4300 万用户账户在 2016 年 9 月被公开发布。这些账户包含有明文形式的用户名、电邮地址和口令。可能是因为该数据已经公开，本次账户数据要价仅 0.0079 比特币 (10.75 美元)。 SunTzu583 的另一份挂单提供了 14.5 万个雅虎账户，售价 0.0102 比特币 (13.75 美元)。这些账户同样包含用户名、电邮地址和被解密的口令。据研究，这些账户来自两次数据泄露，分别为：2013 年 10 月的 Adobe 数据泄露——1.53 亿账户被泄，包含内部 ID、用户名、电邮地址、加密口令及明文口令提示；2008 年的 MySpace 数据泄露——3.60 亿用户账户被盗，2016 年于暗网泄露。
链接地址	http://thehackernews.com/2017/03/gmail-yahoo-password-hack.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.LabSms.a[prv] 2017-03-08	该应用程序包含风险代码，运行过程需要输入手机号码，建议谨慎安装以免造成隐私泄露。（威胁等级高）
	较为活跃的样本	Trojan/Android.Downloader.dg[fra，exp]	该应用伪装成红包助手插件，运行后诱导用户点击下载恶意应用，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.HiddenAds.bj[exp]	该应用运行后会隐藏图标，后台会推送广告，造成用户资费消耗。（威胁等级中）
		Trojan/Android.oxti.y[exp]	该应用运行会隐藏图标，后台频繁访问色情网址，会造成了用户的手机流量损耗。（威胁等级中）
		Trojan/Android.SmsSend.lp[exp]	该应用无实际功能，程序运行后会隐藏图标，私自发送指定短信，造成用户资费消耗。（威胁等级中）
		Trojan/Android.Fobus.b[prv，rog]	该应用伪装成游戏应用 Machinarium（机械迷城），包含广告插件，运行后强制用户通过设备管理器申请，同时存在拦截未接短信、获取用户位置信息等行为，建议卸载。（威胁等级高）
		Trojan/Android.Triada.af[exp]	该程序运行会隐藏图标，私自下载恶意子包，会造成资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.HiddenAds.bk[exp]	该应用为广告插件，运行后会删除自身图标，并推送广告，造成用户流量损失，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	Apache Struts2 存在 S2-045 远程代码执行漏洞 (CVE-2017-5638)	基于 Jakarta Multipart parser 的文件上传模块在处理文件上传 (multipart) 的请求时候对异常信息做了捕获，并对异常信息做了 OGNL 表达式处理。但在在判断 content-type 不正确的时候会抛出异常并且带上 Content-Type 属性值，可通过精心构造附带 OGNL 表达的 URL 导致远程代码执行。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/HTA.Locky	此威胁是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，运行后会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。（威胁等级高）
		Trojan[PSW]/Win32.Adrop	此威胁是一类可以窃取用户密码的木马家族。该家族样本运行后会连接远程服务器接受攻击者恶意操作，收集用户系统敏感信息并回传。（威胁等级中）
		Trojan[Backdoor]/Win32.Qakbot	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后会连接远程服务器接受攻击者恶意操作，包括文件管理，进程查看等。（威胁等级中）
		Trojan[Banker]/Win32.Tuhkit	此威胁是一类可以窃取用户银行信息的木马家族。该家族样本运行后连接远程服务器，收集用户系统中网络银行信息并回传。（威胁等级中）

机器人被黑揭示了新的内部威胁

Kelly Jackson Higgins / 文　安天公益翻译小组 / 译

近日，新的研究表明，机器人及其控制软件充斥着严重和明显的安全漏洞，导致它们很容易被攻击。

IOActive 研究员 Cesar Cerrudo(首席技术官) 和 Lucas Apa(高级安全顾问) 发现，企业、工厂和家庭中使用的热门机器人和机器人控制软件存在约 50 个漏洞，黑客能够利用这些漏洞远程操纵在办公室、工厂或家庭中活动的机器人，渗透其他网络，监控和窃取信息，甚至造成物理破坏。

随着生活及工作的需要，机器人变得“越来越聪明”。其程序设置越来越接近人的行为能力，如面部识别功能。IDC 预测，到 2020 年，全球机器人支出将达到 1880 亿美元。IDC 指出，机器人目前主要用于制造业，但是消费者和医疗保健行业也开始使用机器人。

Apa 和 Cerrudo 研究了相关厂商生产的机器人和其控制软件。他们想在机器人成为主流之前，深入了解其安全问题。机器人及其控制软件存在着不安全的通信漏洞，如机器人及其组件之间的明文或弱加密通信、缺乏身份验证、缺乏授权措施。

此外，他们发现机器人设备及其软件存在弱加密，会导致存储在机器人中的敏感数据和信息面临泄露的风险。一些设备存在弱密码默认配置，用户无法自行锁定它们。Apa 和 Cerrudo 发现，一些设备甚至不支持修改密码，即使遭攻击后修复也无法修改。

Apa 表示：“很难将机器人恢复到初始的未被感染状态。”所以说，一旦机器人被攻击，用户基本上无计可施。

研究结果显示，机器人也遭受一些相同的开源框架以及其他系统软件漏洞库的影响。

IOActive 指出，许多机器人运行 ROS 系统，该系统具有明文通信，身份验证和弱授权等特征。研究人员在报告中写到：“在机器人社区，似乎根据共享软件框架、库、操作系统等，来用于机器人开发和编程是很常见的。如果软件是安全的，这并不是什么坏事。但是，现在的情况并非如此。”

物联网安全专家 Don Bailey 表示，机器人漏洞是嵌入式物联网设备漏洞的另一个例子。“它们都是嵌入式系统，因此相同的威胁会不断地出现。”

他说，今天的机器人设备面临的更大风险是数据和隐私泄露。Amazon Alexa 和 AppleSiri 式智能设备等可以更多地用于间谍活动。“当机器人发展到更实质性的技术时，将会出现更多面向人类的物理危险。”

Bailey 表示，现在的一个严重问题是“机器人如何与其主人关联起来”，当主人将其转给新主人时会发生什么？例如，我们不清楚在前主人能够访问机器人的情况下，新主人该如何保护自己的设备安全。

由于一些设备的费用和全球航运限制问题，研究人员无法测试所有的机器人。所以他们主要分析其软件，包括移动应用程序、操作系统和固件映像。通过对机器人系统的核心元素分析，由此了解其安全问题。目前，研究人员只是初步进行安全审查，他们计划做进一步的分析，更全面地了解目前的机器人安全问题。

Apa 说：“我们认为一些漏洞很容易被利用。任何有手机和应用程序的人都可以通过这些漏洞远程控制机器人，甚至不需要他们自己开发漏洞。”

存在漏洞的产品包括：SoftBank Robotics 的 NAO 和 Pepper 机器人、UBTECH Robotics 的 Alpha 1S 和 Alpha 2 机器人、ROBOTIS 的 OP2 和 THORMANG3 机器人、Universal Robots 的 UR3、UR5 和 UR10 机器人、Rethink Robotics 的 Baxter 和 Sawyer 机器人、Asratec Corp 使用 V-Sido 产品的机器人。

研究人员说，具有面部识别功能的机器人更会被黑客攻击。因为机器人通常带有麦克风和摄像头，所以攻击者可以将机器人用作间谍，窃取信息。“如果攻击者控制了机器人，就可以使用内置的功能来获取机器人识别的面部信息。”Apa 说。

IOActive 不是第一个探索机器人安全问题的公司。2015 年，华盛顿大学攻击了一个医疗机器人，用来演示攻击者如何劫持和控制正在做手术的机器人。

研究人员表示，大多数企业和家庭机器人并无有效的安全保护措 Cerrudo 说：“如果我是一个机器人用户，我会在晚上不用时关掉电源。”

原文名称	Hacked Robots Present a New Insider Threat
作者简介	Kelly Jackson Higgins，Darkreading 的执行编辑，是一位资深技术和商业记者，拥有超过 20 年的报告和编辑经验。
原文信息	2017 年 3 月 1 日发布于 Darkreading 原文地址 http://www.darkreading.com/vulnerabilities---threats/hacked-robots-present-a-new-insider-threat/d/d-id/1328292
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《僵尸网络 Mirai 家族新特性》

近日，安天追影小组持续跟进监控 Mirai 的动态，并对 Mirai 的 BOT 被控端样本进行整理分析发现 Mirai 又有了新的特性。

虽然 Mirai Botnet 还是依旧坚持走 IoT 路线，但是为了获取更多的 IoT 设备进行感染，已经有黑产组织对 Mirai 源码进行改造，将 Scanner 模块分开拓展到了 Windows 系列上，而且 Scanner 在功能上也有所增加，从目前监控到的新版数据分析，Mirai 黑产组织部署该 Windows 版本 BOT 被控端已有一个多月时间。

分析发现，Mirai 家族 Windows Scanner_BOT 主要功能分为 3 个：

1) Telnet 扫描：与 ELF 类型的 BOT 被控端一样，通过自身硬编码内获取 IP 网段进行扫描探测 23 端口的状态，进而解密硬编码的数据获取用户名及密码对开放的端口进行爆破，当爆破成功之后 BOT 被控端则向控制端发送 IP+Port+USR+ PSW。

2) SSH 扫描：SSH22 端口爆破与 Telnet 扫描爆破方法相同，区别是 SSH 的端口号为 22。

3) SQL 扫描：SQL Scanner 主要是 SQL 注入功能，通过 SQL 注入获取的数据价值比 Telnet、SSH 爆破出来数据价值高，因为通过 SQL 注入获取到数据库中的信息中可能连接有大量的 IoT 设备信息，如摄像头、Drv、媒体中心软件及其他内网设备，通过数据库中的设备信息进一步获取其权限并择机向 IoT 设备推送感染 ELF 类型的 Mirai BOT 被控端。SQL 注入功能也是 Mirai 新家族升级后的最大亮点。目前，通过分析发现被注入的数据库类型为微软的 SQL Server 数据库。

Mirai 家族基本包含了 Gafgyt 家族的所有功能特性，Mirai 不仅实现了 Telnet、SSH 网段扫描爆破，而且在此基础上，拓展了指定端口扫描探测如 7547、48101、5555、6789 等，并利用端口服务存在的远程执行漏洞实现 BOT 被控端感染，以及实现拓展到 Windows BOT。

Mirai 家族的魔爪已经不再局限于 Linux 环境，也不再局限于 Telnet、SSH 扫描爆破。该家族已经开始利用 Windows 操作系统潜在的 Botnet 资源环境和 SQL 注入的潜在价值，实现其在 Windows 环境下的传播，而 SQL 扫描注入和 SQL 资源利用有助于 Mirai Botnet 迅速的传播和层次化管控的优化。

对于 Mirai 的防范，不能仅局限于完善 Telnet、SSH 等账号管控，更需要提高对数据库的安全防范，及时更新数据库版本修补漏洞，避免被 SQL 注入。

木马程序

安天【追影高级持续威胁分析系统】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：

文件被网络威胁感知类设备发现，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、静态分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据智能学习鉴定器将文件判定为木马程序。

文件名	93CCD8225C8695CADE5535726B0DD0B6
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	96 KB
MD5	93CCD8225C8695CADE5535726B0DD0B6
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Mirai.a
判定依据	智能学习

根据动态行为（默认环境）得出该文件具有以下行为：通过 http 访问 url、获取计算机名、获取计算机系统版本、运行服务、获取计算机内存信息、dns 请求、获取计算机用户名、提权、疑似桌面控制（字符串扫描）。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
通过 http 访问 url	★	获取计算机名	★
运行服务	★	获取计算机系统版本	★★
dns 请求	★	获取计算机内存信息	★★
疑似桌面控制（字符串扫描）	★	获取计算机用户名	★
提权	★		

报告地址：https：//antiy.pta.center/_lk/details.html?hash=93CCD8225C8695CADE5535726B0DD0B6