安天周观察

主办：安天　2016 年 7 月 18 日（总第 48 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加 2016 阿里安全峰会并发表大会演讲

7 月 13 日至 14 日，以“聚力、赋能”为主题的阿里安全峰会在北京举行。来自网络安全主管部门和职能机构、安全厂商、互联网厂商、高等院校的网络安全专家和爱好者共聚一堂，共话万物互联网时代的网络安全。

安天技术负责人在上午的主会场带来了题为《熊猫的伤痕——中国遭遇的 APT 攻击》的技术报告。他从“威胁是能力和意图的乘积”这一经典名言入手，对“高级、持续、威胁”这三个关键词分别做出新的解读，并以 APT 一词提出者 Greg Rattray 的“旋转门”经历来验证 APT 不是一个纯技术概念，而是一个带有非常复杂化的政治、经济背景，同时又有着非常浓重的大国博弈色彩的概念。他还通过 2015 年安天网络安全年报的数据，解读出中国是受到 APT 攻击最为严重的国家。

安天技术负责人介绍了安天捕获、分析的几例典型的 APT 攻击事件，并以此解读了来自超级大国的“上帝视角攻击”——A^3PT，以及周边地缘利益竞合国家的攻击能力和侵害程度的成长。并讨论了 Cobalt Strike 等商业军火扩散后带来的攻防态势影响。与在此前一次安全会议上安天的同名报告相比，本次报告对方程式、白象等攻击事件增加了信息披露。其中白象事件补充了安天刚刚发布的报告的最新内容。他坦诚地表示，目前安天的多数分析工作还依然停留在对“弹头”的分析，而对“兵工厂”、“狙击手”还缺乏有效的分析。但弹头的分析即是直接的工作，也是必须的工作，否则反 APT 是难以有效展开的。

但安天技术负责人同时也指出，APT 分析工作的核心价值不是为了发布报告，而是为了实现更有效的“防御”、更彻底的“止损”。在讨论 APT 解决之道时，他认为，当前首先要做的是确保基础 IT 环境和基本功到位，这样一些高阶手段和能力才能有效对接。同时，单点能力和手段都是不足以迷信。他认为：IOC 信标等威胁情报，在面对当前载体加载方式和隐蔽通讯手段时能力在打折扣。而白防，不能只有白名单，而必须要有可靠的主动防御来改善入口控制。反病毒引擎正在从一个单独的“表决器”，走向一个深度静态向量提取装置。而沙箱绝非是可以“安装后不管”的智能设备，只有网络管理者和厂商提供持续的观测和关联分析，才能避免其成为摆设。

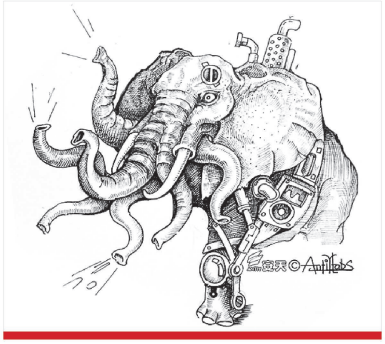
安天技术负责人最后指出，一个国家的反高级威胁能力，需要跳脱出保护目标的本身，要以产业生态、供应链和信息流为基础来建立。

他以：“这是我们的土地、天空、海洋和网络空间”，“不义之财分文不取，祖宗之地寸土不让”，作为了演讲结束语。

安天发布《白象的舞步——来自南亚次大陆的网络攻击》分析报告

近日，安天发布了《白象的舞步——来自南亚次大陆的网络攻击》分析报告，披露了两组针对我国多领域的高频度 APT 攻击事件。安天对这一系列针对中国教育、科研、军事等领域的攻击行动，进行了近四年时间的持续监测、捕获、跟踪、分析，确定这些攻击来自南亚次大陆的某个国家，并将报告中的两组攻击统称为——“白象行动”。

在报告中，于 2012 年—2013 年被发现的这组攻击被称为“白象一代”，其未使用复杂的



加密算法，也未使用 0day 漏洞和 1day 的漏洞，更多的是采用鱼叉式网络钓鱼攻击，所以其被划分为轻量级 APT 攻击。2015 年年底被发现的这组攻击被称为“白象二代”，其摆脱了白象一代杂乱无章的攻击手法，整体攻击行动显得更加正规化和流程化，至少使用了 CVE-2014-4114 和 CVE-2015-1641 等三个漏洞，可以说白象二代的攻击次数和影响范围远远超过了白象一代。（完整报告：http://www.antiy.com/response/WhiteElephant/WhiteElephant.html#rd）

每周安全事件

类 型	内 容
中文标题	Anonymous 黑客组织曝光南非武器采购部门机密数据
英文标题	Anonymous Leaks Data from South Africa's Arms Acquisition Agency
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，匿名者黑客组织 Anonymous 入侵了南非官方武器采购机构 Armscor，泄漏了大量的机密数据。攻击者曝光了 Armscor 公司采购管理系统的控制界面截图，以及机构官员的个人信息、客户的财务数据、相关的武器采购交易明细等数据。除了武器采购信息之外，此次泄漏的数据库中还包含有其他供应商的采购信息，例如：西门子、波音公司、BAE 系统公司、萨博公司、欧洲航空防务与航天公司、劳斯莱斯、松下、格洛克技术、泰利斯航空、微软以及南非丹尼尔公司等众多技术供应商。
链接地址	http://news.softpedia.com/news/anonymous-leaks-data-from-south-africa-s-arms-acquisition-agency-506213.shtml

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.FakeFarMap.a[prv]2016-07-12	该应用程序运行后会通过私发短信窃取手机固件信息，建议及时卸载。（威胁等级低）
		Trojan/Android.Vibleaker.a[prv，fra]2016-07-12	该程序伪装成游戏应用，后台获取用户 viber 图片、缓存图片及视频上传到指定服务器，造成用户隐私泄露和资费损耗，建议不要安装。（威胁等级低）
		G-Ware/Android.qyPay.a[rog，pay]2016-07-14	该游戏应用运行后存在不明显的提示信息，以领取道具的名义诱导用户点击进行付费操作，造成用户资费损耗，同时还具有短信拦截、删除等行为，建议立即卸载。（威胁等级低）
		Trojan/Android.whatsspy.a[prv，rmt，spy]2016-07-14	该应用是一款间谍应用，具有隐藏图标、激活设备管理器和 root 功能，能够接收指令，获取用户程序列表信息、浏览器历史记录、通话记录、联系人、短信等隐私信息上传到服务器，造成用户隐私泄露，如非自主安装建议及时卸载。（威胁等级高）
		Trojan/Android.Trackop.a[prv，fra]2016-07-14	该程序伪装成系统应用，运行后开启 GPS 获取用户地理位置信息和手机固件信息，执行上传操作，通过监听手机指令获取实时地理位置信息，造成用户隐私泄露，建议及时卸载。（威胁等级中）
	较为活跃的样本	G-Ware/Android.Ventica.b[rog，exp]	该应用运行后会隐藏图标，在通知栏显示浏览器搜索框，点开后是包含多个色情网址的浏览器，会安装桌面快捷图标，可能会私自下载 apk 应用，造成用户资费消耗。（威胁等级低）
		Trojan/Android.E4AQQspy.h[prv，exp]	该程序伪装成 QQ 悄悄话查看器，窃取用户账号密码和收件箱内容，并通过短信转发，建议立即卸载，避免造成隐私泄露和资费损耗。（威胁等级高）
		Trojan/Android.QQspy.k[prv，exp]	该应用程序伪装成 QQ 应用，运行后联网上传用户登陆账号和密码，后台获取手机短信箱、通讯录、地理位置以及手机相册等信息，造成用户隐私泄露，建议及时卸载。（威胁等级高）
		Trojan/Android.SmsThief.aj[prv，exp]	该应用伪装成系统应用，运行后隐藏图标，私自发送短信，监听短信，拦截短信并将短信信息转发到指定号码，造成用户隐私泄露和资费消耗。（威胁等级高）
		G-Ware/Android.Fakekugou.a[rog，exp]	该应用伪装成酷狗播放器，弹窗诱导用户下载应用并在后台静默安装，频繁加载广告，造成用户资费损耗，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 内存破坏漏洞 (CVE-2015-1641)	攻击者可以构造嵌入了 docx 的 rtf 文档进行攻击。word 在解析 docx 文档处理 displacedByCustomXML 属性时未对 customXML 对象进行验证。（威胁等级中）
	较为活跃的样本	Trojan[Downloader]/JS.Nemucod	此威胁是一种木马家族，该家族样本是 js 脚本，运行后连接远程服务器下载恶意代码并执行，可能会窃取用户信息，造成一定威胁。（威胁等级中）
		Trojan[Ransom]/Win32.Radam	此威胁是一种木马家族，该家族样本运行后会加密用户文档并要求其支付一定费用，只有按时付费的用户才可以解密文档。（威胁等级中）
		Trojan[Ransom]/Win32.Locky	此威胁是一种木马家族，该家族样本运行后会加密多种格式文件，并勒索用户支付比特币解锁，造成一定威胁。（威胁等级高）

物联网医疗器械堪称灾难

Tom Spring / 文　安天公益翻译小组 / 译

如果你病了，坐在单调的病房里，身上连着透析泵，你最不希望发生的也许就是黑客攻击。但是 IT 医疗安全专家指出，挽救生命的透析机可能会被恶意软件感染，甚至可以用来处理欺诈性信用卡交易，或者沦为 DDoS 攻击的一部分。

Cyber Risk Management 首席执行官 Yong-Gon Chon 表示，现在医院已经成为了黑客的主要目标之一，连网的医疗设备对于黑客来说唾手可得，他们能够通过窃取病历和计算机资源或者执行勒索软件攻击来快速赚钱。

Chon 表示：“物联网医疗设备可以挽救生命，但其不能像笔记本电脑那样离线，返回 IT 部门花费一周的时间进行擦除和重新映像。”同时，Chon 还指出，现代医院安防系统往往忽视了物联网设备的安全性，导致它们很容易遭到攻击。

上月末，TrapX Labs 的安全团队发现一个新的恶意软件家族攻击医院及其物联网设备的事件剧增。研究人员发现，攻击者针对运行 Windows XP 和 Windows 7 系统的未打补丁的医疗设备执行各种被认为过时的攻击，例如 Conficker 蠕虫等。TrapX Labs 表示，该恶意软件提升了功能，能够在网络中横向运动，攻击具体类型的医疗设备，这些设备很可能连接到后端医

疗记录系统。

TrapX Labs 的联合创始人 Moshe Ben-Simon 说：“利用不受保护的放射设备作为据点，黑客能够跳转到医院的中央服务器。”他还表示，目前大多数医院的医疗设备在设计时没有优先考虑安全性。他说：“它们的使命是拯救生命，而非对抗网络攻击。一旦物联网设备部署完毕，再添加安全措施就没那么简单了。”

如果你认为医院物联网设备的保护措施欠佳，更糟的还在后头。在最近的一项研究显示，当涉及基本的网络安全实践时，医生、护士和医院 IT 人员的得分都不及格，这进一步恶化了已经处于不利地位的医院安全防御。

该研究发现，医生不愿意打破旧的工作流程，或采取最基本的网络安全做法，如双因素身份验证或基本密码。报告指出：“我们发现用户随处写下密码，例如医疗设备上和配药室中的便签都会出现用户名和密码。”

同时，医院病历被盗事件也是一个噩梦。根据美国卫生和人类服务部的数据，仅在 2015 年就有超过 1.13 亿医疗记录被窃取。上月的一份报告称，一名黑客在暗网上出售 65.5 万份医疗记录。在接下来的一周，这一数字激增，并且该黑客声称来自一家医疗保险提供商的 930 万份病历即将上线。同时，在之前的一个月，佛罗里达州的癌症治疗中心 21st Century Oncology Holdings 警告 220 万病人，其医疗数据和社会安全号码被窃取。

为什么黑客将注意力从信用卡数据转向了医疗记录。首先，因为医院的安全措施更少，更容易窃取其数据。但更重要的原因是，医疗记录数据包含姓名、出生日期、社会安全号码和医疗信息，其价值远远超过信用卡数据。

TrapX Labs 指出，在暗网上，每份医疗记录的售价为 20-40 美元，而每份信用卡记录的售价为 5 美元左右。医疗记录能够用于各种不同的诈骗，包括传统的金融身份盗窃，伪造的手术、治疗或处方账单等。TrapX Labs 表示，他们正在与医疗欺诈预防公司合作，防止攻击者利用窃取的医疗记录购买昂贵的药物，然后在黑市上倒卖。

原文名称	IoT Medical Devices：A Prescription for Disaster
作者简介	Tom Spring，Threatpost 副主编。
原文信息	2016 年 7 月 11 日 Threatpost 发布，原文地址 https://threatpost.com/iot-medical-devices-a-prescription-for-disaster/119155/
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《DDoS 攻击之鬼影 DDoS 家族分析》

近日，安天追影小组发现了大量的鬼影 DDoS 家族变种，并在进行网络通信流量监控时发现，异常通信行为中占比最大的正是鬼影 DDoS 家族，安天追影小组随即对其进行了分析。

1. 样本分析

1）样本运行后会在系统目录下释放以 6 为随机字符为名称的 PE 文件，并创建该名称的进程，还会为其创建特定服务名称的服务项，以完成自身自启动的目的。

2）创建互斥量，互斥量大多情况与服务名相同。

3）释放名称为 hra33.dll 或 gei33.dll 的文件，同时在所有系统应用程序目录下释放其复制体，名称为 lpk.dll，用以劫持系统 lpk.dll 文件。

4）有些变种还会开启线程对局域网的主机进行弱密码猜解，猜解成功后会直接自复制到目标主机的共享目录中（admin$\C$\D$\E$\F$），然后去感染局域网其他用户。

5）一些变种也会使用到 Rootkit、不死进程等方式存活。

6）完成感染主机后，样本就会开启线程与 C2 进行通信，并根据接收的命令进行相关的操作。

2. 解决方案

1）查看进程列表和系统目录 C:\Windows\System32 或 C:\Windows 目录下，是否有随机以 6 为字符为名称的进程和文件。关闭进程，删除文件。

2）删除相应的服务项。

3）下载系统 lpk.dll 文件，替换到 C:\Windows\System32\lpk.dll，并删除系统中其他所有 lpk.dll 文件，及 gei33.dll 或 hra33.dll 文件。

4）由于手动删除较为麻烦，建议用户更新杀毒软件病毒库，并定期检测。

3. 总结

经分析，黑客利用包括鬼影 DDoS 家族在内的 DDoS 恶意代码进行攻击时，大多会采用阶段性攻击方式，一般表现为受害端机器暂时卡顿一段时间，使受害者认为是网络问题，而不会意识到自身机器被感染，从而增强了恶意代码的生存周期。

同时，DDoS 攻击对网络财产、隐私等内容进行窃取，并从中获利，在利益的驱动下，DDoS 攻击业务必然快速滋生，对政府单位、企业、事业、个人等正常服务网站和其他网站系统造成巨大的威胁，对网络安全环境造成极大的危害。安天建议广大用户加强网络安全防护意识，定期更新杀毒软件病毒库，对此类威胁进行检测查杀。

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：

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、YARA 自定义规则鉴定器、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 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、动态行为鉴定器、智能学习鉴定器将文件判定为木马程序。

该文件具有以下行为：疑似 Trojan/Win32.Dufeva.dfiddos、启动服务、自启动、创建服务、复制文件到系统目录、释放 PE 文件、获取驱动器类型、打开自身进程文件、获取 CPU 信息、疑似桌面控制。

文件名	FE142A9BBC3A85E66C2E289358554505
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	58 KB
MD5	FE142A9BBC3A85E66C2E289358554505
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Dufeva.dfiddos
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=FE142A9BBC3A85E66C2E289358554505

◆ 危险行为

行为描述	危险等级
疑似 Trojan/Win32.Dufeva.dfiddos	★★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
启动服务	★	自启动	★
创建服务	★	复制文件到系统目录	★★
获取驱动器类型	★	释放 PE 文件	★
获取 CPU 信息	★★	打开自身进程文件	★
疑似桌面控制	★		