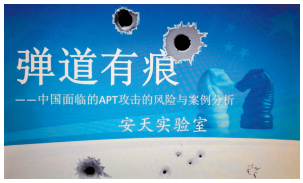
# 安天周观察

主办：安天　2015 年 12 月 7 日（总第 19 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

## 安天参加自主可控沙龙并发表主题演讲

2015 年 12 月 5 日，来自 20 多个单位网络安全与保密战线的技术人员自发组织并参加了“自主可控第一期沙龙”活动。安天参加了此次活动并发表了题为《弹道有痕——部分中国遭遇到的网络攻击分析》的主题演讲。




安天技术负责人从解读中国“网络安全”地缘因素入手，指出了当前的威胁向纵深延展和泛化演进的趋势。重点介绍了安天从 2010 年来，分析震网、火焰、方程式、Hangover、APT-TOCS 等事件的经验，并针对不同的攻击者的攻击能力、攻击特点做了评价和总结。

在报告中，针对如何有效发现、遏制相关攻击，提出了自身的观点。包括如何建设纵深防御策略和增加新的布防点问题。建议将削弱、干扰、阻断攻击链作为防御工作的主导思路，也分享了安天如何利用自身所擅长的流量侧的还原捕获与回溯能力、基于沙箱的深度检测、白名单 + 安全基线等产品能力，与用户安全策略即既有防火墙、企业级杀毒产品如何有效融合，提出了相关建议。


安天以可视化方式复现中方某机构遭遇到的攻击

## 恶意软件『玻璃老鼠』隐藏数年之久专门攻击中国

近日，一个隐藏数年之久的远程访问木马“GlassRAT”（玻璃老鼠）被公布，其目标是与跨国公司有联系的中国公民。至少在 2012 年，玻璃老鼠就已被部署在网上，由于它的安装器是用从中国盗来的合法证书签名，直至今年 9 月它才被公共恶意软件数据库收录。玻璃老鼠具备典型的木马特征，包括用来帮助攻击者访问受感染设备的反向 shell。玻璃老鼠的部分代码与名为 Taidoor 的恶意软件非常相似。后者主要被网络间谍组织使用，目标是各国政府机构、企业及智库。（文章来源：http://www.aqniu.com/news/12090.html）

## 安天举办『文档秘籍』培训

为了帮助安天员工建立正确的文档意识，培养良好的文档习惯，形成自己的工作方法。12 月 3 日，安天哈尔滨总部举办了一场实用性极强的文档培训。本次培训以“5W1H”为主题，培训讲师结合具体案例，详细讲解了如何使用 5W1H 来理清问题的本质。12 月 9 日，信息开发管理组将再次举办培训，讲解安天文档秘籍之“用思维导图延伸思维路径”。

## 2015 年第四季度 Cybersecurity Ventures 网络空间 500 强企业名单公布 中国厂商排名全面下滑

近日，Cybersecurity Ventures 公布了 2015 年第四季度的网络空间 500 强企业名单 (The Cybersecurity 500 List for Q4 2015)，与前三次评选相比，中国网络安全厂商的排名明显下滑，且上榜厂商从四家减少到三家。其中之前一直处于百名之内的安天本次下滑至 205 名，但仍是排名最为靠前的中国厂商。

安天此次排名下滑可能与安天在海外业务的缩紧策略有关。安天从检测引擎供应商目前正在快速转型为 APT 检测与威胁预警解决方案的供应商，并面向国内市场完成了企业安全、移动安全的两翼布局，新的产品体系已经成型，等待发力。

另外，针对中国厂商排名的全面下滑，有媒体分析认为，从大环境来看，也反应出在美国供应链审查压力下，中国安全厂商在国际市场的普遍业务收缩和对应的影响力被削弱。

# 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | 安卓恶意软件 Shedun 回归影响大量安卓用户 |
| 英文标题 | Shedun adware can install any malicious mobile app by exploiting Android Accessibility Service |
| 作者及单位 | Pierluigi Paganini，Security Affairs |
| 内容概述 | 近日，安全人员发现，即便有些用户已经明确拒绝了界面跳转出来的安装请求，一些 Android 广告软件仍旧会自行开始安装。这些广告软件出自一个叫做 Shedun 的家族，包括 Shedun(GhostPush)、Kemoge(ShiftyBug)、Shuanet。Shedun 利用系统服务中的合法功能，通过获取许可使用可访问性服务读取屏幕上出现的文本信息，然后当屏幕上出现安装窗口时再决定是否安装该软件。目前，Shedun 直接将自己植入到设备中并嵌入系统分区里边，即使用户在使用设备时恢复出厂设置功能，该种恶意软件依旧不会消失。 |
| 链接地址 | http://securityaffairs.co/wordpress/42164/malware/shedun-trojanized-adware.html |

# 每周值得关注的恶意代码信息

经安天检测分析，本周 10 个移动平台和 5 个 PC 平台的恶意代码家族值得关注

| 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 | Trojan/Android.emial.a[prv，rmt，fra] 2015.11.26 | 该应用程序伪装成其他应用的插件，安装运行后，激活设备管理器，删除图标，在后台私自发送短信到指定号码，执行短信指令，窃取用户短信息内容，造成用户隐私泄露和资费损失。( 威胁等级中 ) |
| | | Trojan/Android.zthml.a[pay，fra] 2015.11.27 | 该应用伪装成系统程序，开机自启，联网上传手机固件信息，获取配置信息，执行私发短信、屏蔽删除指定短信、自动回执短信等操作，给用户带来经济损失，建议卸载该应用。( 威胁等级中 ) |
| | | Trojan/Android.DexSync.a[exp，rog] 2015.11.29 | 该应用程序安装无图标，触发启动后会释放子包，后台私自联网下载未知 apk 文件然后静默安装并隐藏图标，同时将下载网址存入浏览器书签中并创建快捷方式，造成用户资费损耗，建议立即卸载。( 威胁等级中 ) |
| | | AdWare/Android.ninebox.a[ads] 2015.11.29 | 该应用捆绑了 ninebox 广告件，会采用通知栏弹窗方式，弹出广告，可能对用户正常体验造成影响，建议谨慎使用。( 威胁等级低 ) |
| | | Trojan/Android.YmSdk.a[prv，exp] 2015.11.29 | 该应用伪装成系统应用，运行时释放子包加载广告，获取并上传，用户手机固件信息；搜集用户应用安装数据并上传；静默安装应用，造成用户隐私泄露和资费损失，建议立即卸载。( 威胁等级高 ) |
| | 较为活跃的样本 | AdWare/Android.dyds.d[ads] | 该应用包含 dyds.d 广告插件，运行时会自动获取 IMEI 和 IMSI，可能会造成用户隐私泄露。( 威胁等级低 ) |
| | | Trojan/Android.Tiak.b[exp，rog] | 该应用安装无图标，监听广播开机自启动，私自下载恶意应用，并通过监听手机行为释放广告，建议用户立即卸载。( 威胁等级中 ) |
| | | RiskWare/Android.InfoStealer.d[prv] | 该应用程序运行后，在用户不知情的情况下获取用户手机号码，imei 私自上传到远程服务器上，给用户造成一定的隐私泄露。( 威胁等级低 ) |
| | | Trojan/Android.SettingSpy.a[rmt，prv，spy] | 该应用安装无图标，运行后会接收短信指令来获取用户短信、联系人、通话记录、浏览器浏览历史等信息，并存储在本地，通过短信将内容反馈到远程号码，删除短信、删除联系人、删除通话记录。( 威胁等级中 ) |
| | | Trojan/Android.Fakegupdt.y[rog，exp] | 该应用程序伪装成游戏及笑话应用，实际安装无图标，后台发送订阅短信，下载 apk。通过通知栏伪装系统更新，诱导用户点击安装。后台拦截指定短信消息并自动回复，造成用户资费损耗，建议立即卸载。( 威胁等级中 ) |
| PC 平台恶意代码 | 活跃的格式文档漏洞、0day 漏洞 | Microsoft 文字本地区域远程执行代码漏洞 (CVE-2015-0097) | Microsoft Office 软件中存在的一个远程执行代码漏洞，该漏洞源于程序分析经特殊设计的 Office 文件时，没有正确处理内存对象。攻击者可通过诱使用户使用 Microsoft Office 的受影响版本打开经特殊设计的文件，利用该漏洞执行任意代码，从而损坏系统内存。( 威胁等级中 ) |
| | 较为活跃样本 | Trojan[PSW]/Win32.Glacier | 此威胁是一种木马类程序。该恶意代码会搜索系统中的有用信息，并通过 QQ 信箱进行上传。( 威胁等级中 ) |
| | | Trojan/Win32.Winlagons.ae | 此威胁是一种木马类程序，运行后会劫持浏览器，使用户访问黑客指定网站，下载恶意程序。通过不断下载恶意程序到被感染计算机中，使其系统无法承受巨大的资源占用，导致系统崩溃。( 威胁等级中 ) |
| | | Trojan[Downloader]/Win32.Tintin | 此威胁是一种木马类程序。运行后会添加注册表启动项，实现自身随机启动，与指定的远程服务器连接，下载其他恶意软件到本地运行。( 威胁等级中 ) |
| | | Trojan[Downloader]/Win32.CcKrizCry | 此威胁是一种木马类程序。通过网站下载进行传播，多为 IE 安装程序，但在安装过程序中会去网络上下载游戏、播放器等其他恶意程序。( 威胁等级中 ) |

# 医生寻求拯救医疗设备免遭黑客攻击

Kim Zetter/ 文　　安天公益翻译小组 / 译

物联网使曾经安全的家电变成了数据窃取和监控的网关。但令人更为不安的是，物联网创造了一套全新的可带来生命危险的安全漏洞，比如医疗设备漏洞，包括药物输液泵，心脏起搏器，以及其他关键的医院设备。

读过安全研究人员的报告之后，米尔斯半岛健康服务糖尿病研究所的内分泌专家和医疗主任大卫·科洛诺夫博士对于病人的安全非常担忧。这些漏洞允许黑客操纵胰岛素泵，导致患者的血糖直线下降，导致病人陷入糖尿病昏迷或死亡。“现在，任何医疗设备都没有安全标准。”科洛诺夫指出，“作为医疗保健专业人士，我们希望看到患者有安全的设备，而不是处于危险之中。”

然而，创建胰岛素泵安全标准面临着挑战。在设备中加入指纹识别和密码验证，可能会导致病人无法使用自己的设备，比如说他的手指湿了或者忘记了密码。科洛诺夫希望找到一种方法，确保胰岛素泵阻断恶意黑客；同时还允许患者破解自己的胰岛素泵，从而实现更好的结果。

目前市场上的一些糖尿病系统存在漏洞，这是厂商遗留在固件中的一个调试功能，患者一直利用该漏洞来创建自己的闭环系统。他们自创的系统使用复杂的算法来评估血糖监测仪的读数，自动确定适当的胰岛素剂量，并指示胰岛素泵提供相应的剂量。该算法甚至可以根据计划的活动和生活方式预测胰岛素需求量。

本·韦斯特是一名计算机工程师。他花了几年时间研究自己的胰岛素泵的软件，想弄清楚怎么自动读数血糖监测仪，进行计算并向胰岛素泵发送命令。他在 GitHub 博客中记录了这一过程。在他的研究过程中，他反编译了胰岛素泵系统中使用的核心代码，并在网上进行公布，这使得两个糖尿病患者的父亲和丈夫布莱恩·玛兹丽施设计了一个闭环系统，并由此创建了 Bigfoot BioMedical 公司。但是，这一商业系统短期内无法上市。因此，韦斯特和西雅图的一对夫妇创建了一个名为 OpenAPS 的工具包，集成了不同的糖尿病监测软件和泵组件的各种数据集，使他们能够通信。用户要想安装，需要进行一些细化，但是，它能够与多个血糖监测系统协作。


这种破解给一些患者的生活质量带来了巨大的改变。克里斯·哈尼曼是一位 31 岁的机械工程师，8 岁时被诊断为 I 型糖尿病。哈尼曼的姐姐也患有 I 型糖尿病，而他的父亲患有 II 型糖尿病。

使用韦斯特开发的工具，哈尼曼破解了他的 Medtronic Mini Med Paradigm 723 胰岛素系统，“当你进食或者血糖太高想做调整时，你可以告诉胰岛素泵立即或过一段时间给予较大剂量。”他说，“这是你无法从目前的任何商用系统中找到的东西。我可以提取本来无法获取的数据，并做些很细微的调整，这些只能靠适合自己治疗的定制设备完成。使用这个工具，我得到了更好的健康结果。”

虽然自动化系统最终将会上市，但是，哈尼曼和其他人都不愿意等待。“这是我们的捷径，我们能够用这种方式控制目前市场上的设备。”哈尼曼说。大约两个月前，他和韦斯特与科洛诺夫取得了联系，并提供了建议。“作为患者，我们有一个独特的视角。我们是病人，但我们可能正好是边沿病例患者。”他说。

哈尼曼说，胰岛素泵安全标准面临的挑战并不意味着安全性与封闭划等号。“你真正想拥有的是一个所有传输都安全的系统，你希望设备和胰岛素泵之间进行数字握手，从而进行验证，而且你希望不同的验证等级。这样一来，第三方设备可以从胰岛素泵读取数据但是不会向它发送命令。”他说，“我想要这样的第三方设备，这样，只有我的设备可以与胰岛素泵进行加密通信。我不希望别人与我的胰岛素泵进行通信。”

科洛诺夫同意了他们的建议并说，胰岛素泵安全标准应该将韦斯特、哈尼曼和其他人的 DIY 活动纳入考虑，因为他们的修修补补已经为自动胰岛素泵的创新做出了重大的贡献，而且会引导出更多的创新，为患者带来福音。

| 原文名称 | The Doctor On A Quest To Save Our Medical Devices From Hackers |
|---|---|
| 作者简介 | Kim Zetter，《连线杂志》一位屡获殊荣的资深记者，研究范围包括网络犯罪、隐私和安全。 |
| 原文信息 | 2015 年 11 月 24 日《连线杂志》发布<br>原文地址 http://www.wired.com/2015/11/the-doctor-on-a-quest-to-save-our-medical-devices-from-hackers/ |
| 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。<br>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《邮件发送 JS 脚本传播敲诈者木马的分析报告》

安天威胁态势感知系统 2015 年 12 月 2 日捕获到有新的传播特点的敲诈者变种邮件，其不再采用直接发送二进制文件载荷的传播模式，而是以一个存放在压缩包中的 JS 脚本为先导。

安天追影分析小组对相关事件和样本进行了分析。该样本系 TeslaCrypt 的另一个变种 TeslaCrypt 2.x，邮件附近是一个 zip 压缩文件，解压 zip 文件得到一个 js 文件，运行 js 文件，会下载 TeslaCrypt2.x 运行，遍历计算机文件，对包括文档、图片、影音等 186 种后缀格式文件进行加密，加密完成后打开敲诈者的主页，在指定期限内需要支付 500 美元才能得到解密密钥，过期需要支付 1000 美元。

因为 TeslaCrypt2.x 变种改变了密钥的计算方式，采用了 ECDH 算法，黑客与受害者双方可以在不共享任何秘密的情况下协商出一个密钥，采用此前思科等厂商发布的 TeslaCrypt 解密工具已经无法进行解密。

敲诈者软件此前通过邮件打包传播可执行 PE 载荷，通过双扩展名、SCR 扩展名等技巧进行传播，而在这一轮传播攻势中，其利用 js 格式的伪装性，逃避杀软的检测和防御。同时，特斯拉 2.x 敲诈者采用 ECDH 加密算法，其已经无法再通过此前的逆向获取密钥的方式来解密文件，对用户的数据安全，具有更大的威胁。

从我们过去的监测发现，敲诈型恶意代码的威胁对象，的受害对象，正在从原有的个人用户，广泛的延伸到企业用户，甚至出现了服务器被感染的案例。安天已经在 PTD 探海威胁检测系统、IEP 智甲终端防御系统中，专门强化了对敲诈者木马的检测防御能力。

随着数据安全威胁日益增长，行业企业用户同样需要通过能力型网络安全产品有效改善感知防御盲区，建立纵深防御体系，并通过威胁情报平台及时获取威胁信息。快速发现威胁，降低风险进一步扩散。

## 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，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、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。

依据动态行为鉴定器最终将文件判定为木马程序。

该文件具有以下行为：

| | |
|---|---|
| 文件名 | 0352ACD36FEDD29E12ACEB0068C66B49 |
| 文件类型 | Text/Script.Javascript |
| 大小 | 6 KB |
| MD5 | 0352ACD36FEDD29E12ACEB0068C66B49 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan[:RAT]/Win32.SGeneric |
| 判定依据 | 动态行为 |

◆ 危险行为

| 行为描述 | 危险等级 |
|---|---|
| 调用 bcdedit 修改启动环境 | ★★★★ |

调用 bcdedit 修改启动环境；请求调试权限；填充导入表 ( 疑似壳 )；释放 PE 文件；增加 run 自启动项；文档篡改；获取系统版本；打开自身进程文件；访问文件尾部；获取计算机名称；结束进程；复制自身文件；创建特定窗体；获取驱动器类型；独占打开文件；遍历进程；获取主机用户名称；请求加载驱动的权限。

◆ 其他行为

| 行为描述 | 危险等级 | 行为描述 | 危险等级 |
|---|---|---|---|
| 请求调试权限 | ★ | 填充导入表 ( 疑似壳 ) | ★★ |
| 释放 PE 文件 | ★ | 增加 run 自启动项 | ★ |
| 获取系统版本 | ★ | 文档篡改 | ★★ |
| 访问文件尾部 | ★ | 打开自身进程文件 | ★ |
| 复制自身文件 | ★★ | 获取计算机名称 | ★ |
| 获取驱动器类型 | ★ | 结束进程 | ★★ |
| 独占打开文件 | ★ | 创建特定窗体 | ★ |
| 遍历进程 | ★ | 获取主机用户名称 | |
| 请求加载驱动的权限 | ★ | | |

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=0352ACD36FEDD29E12ACEB0068C66B49