# 安天周观察

主办：安天　2016 年 12 月 12 日（总第 68 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流


## 2016 年度会员大会在京召开 中国网络安全产业联盟

12 月 3 日，中国网络安全产业联盟 2016 年度会员大会在京召开。中央网信办网络安全协调局副局长胡啸出席大会并致辞。国内网络安全专家及联盟会员单位 300 余名代表参加了会议，安天作为中国网络安全产业联盟常务理事单位参会。

本届会议由中国网络安全产业联盟秘书长陈兴跃主持。大会听取了陈兴跃秘书长关于《联盟 2016 年工作总结的报告》、《2017 年工作设想的报告》，表决通过了《关于修改中国网络安全产业联盟章程的提案》。会上，根据会议章程及选举办法，选举产生 12 家新增理事单位，选举出的理事单位将与 32 家发起单位理事共同组成联盟理事会。

在随后举行的联盟第一届理事会第三次会议上，理事长、常务理事、新当选理事代表及发起单位理事代表分别发言，就联盟 2017 年度工作内容提出建议，并表达了对联盟工作的期望。

目前，中国的网络安全事业已经有了长足的进步，但相对于保障网络强国的屏障使命，以及保护网络空间人类命运共同体的愿景价值，各企业都任重道远。联盟成员更需要抱团取暖，携手成长为网络空间的中国产业森林。

今后，中国网络安全产业联盟将继续致力营造良好的网络安全产业发展环境，保障国家网络安全和用户利益，为推动我国网络安全产业做大、做强和维护国家网络空间安全而不懈努力。

安天作为常务理事单位之一，也将加强企业自律，遵守联盟章程，积极配合联盟各项任务和工作，为维护国家网络安全和用户信息安全贡献一份力量。

## 安天获中央网信办感谢函

近日，为表彰安天在第三届世界互联网大会（乌镇峰会）期间所做工作，中央网络和信息化领导小组办公室国际合作局特向安天发来感谢函。

在第三届世界互联网大会（乌镇峰会）会议期间，经大会组委会高级别专家咨询委员会审议通过并发布的《2016 年世界互联网发展乌镇报告》（以下简称《报告》）成为本届大会的标志性成果，安天有幸参与了《报告》的起草、修改等工作。

中央网信办对安天的工作给予了肯定，并在感谢函中提到：“安天在《报告》的起草、修改及大会期间专项工作中，扎实推进相关工作，高质、高效的完成各项任务，体现了安天突出的专业水平和和严谨的工作态度，为《报告》的最终发布做出了重要贡献。”

安天经过 16 年的发展，技术实力已得到行业管理机构的认可。现在，安天正积极地支持国家网络安全建设，坚持自身产业责任和基础能力建设，曾多次收到来自行业主管部门的书面感谢。

## 安全新闻

### ◆ 日本化妆品牌资生堂确认 42 万用户数据泄露

近日，日本化妆品巨头之一的资生堂公司宣称数据遭泄露，所泄露数据涉及到 42 万用户，其中，包括他们的财务信息。日本媒体曾在近期爆料，资生堂公司遭遇黑客攻击，数据也因此泄露。紧接着，资生堂公司宣布，黑客通过入侵公司的在线商城来窃取数据。这个商城由资生堂的子公司 IPSA 运营。

该公司透露，黑客大约接触到了 42 万用户的个人信息，这些信息有可能已经泄露。

日本媒体提到：“本次所泄露的数据包括用户的姓名和地址。同时，IPSA 公司也确认一部分用户的财务信息被泄露了。除此之外，还有多达 5.6 万用户的信用卡信息也可能被窃漏。”

IPSA 还提到，在 2011 年 12 月 14 日至 2016 年 11 月 4 日期间，如果用户曾在 IPSA 在线商城购物，那么他们的账户信息都面临泄露的风险。（来源：http://www.cnnvd.org.cn/news/show/id/7950）

### ◆ 防黑客入侵，惠普停用远程访问网络打印机

近日，惠普宣布了一项新的决定，停用商用打印产品的远程访问支持，其中包括 FTP、Telnet 等。其实，不少用户都习惯了远程访问打印机这种方式。

据悉，惠普的这项决定暂时针对准备上市的新产品。他们也害怕再次引发类似上次停用第三方墨盒时外界的愤怒。惠普表示新产品的远程访问将默认关闭，如用户需要，依然可以激活（预计隐藏很深或者需要专门的驱动）。同时，对于现有产品，惠普也宣布将升级固件，加强了通讯协议的口令密码和安全认证。

惠普最后强调，他们正在将无线打印机的易用性扩展，以便替换掉传统的 FTP 和 Telnet。（来源：http://www.cnnvd.org.cn/news/show/id/7960）

# 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | 索尼 80 款监控摄像头存秘密后门 |
| 英文标题 | Sony kills off secret backdoor in 80 internet-connected CCTV models |
| 作者及单位 | Pierluigi Paganini；Securityaffairs |
| 内容概述 | 近日，索尼生产的约 80 款网络摄像头中存在硬编码的登陆凭证信息。由于其是静态的身份凭证，一旦被破解，就可以被 Mirai 等恶意软件用来控制设备，从而发动大规模的 DDoS 攻击。这些存在漏洞的摄像头都来自 Sony Professional Ipela Engine 系列的 IP 摄像头。<br>这些摄像头都是索尼针对专业市场生产的安全摄像头，价格都比较高，用户群体主要是企业和政府机关。上文提到的硬编码身份凭证信息，本质上可以算是“秘密后门”。奥地利信息安全公司 SEC Consult 的 Stefan Viehböck 于近期发现了该后门，并对外公布了研究报告。索尼官方表示已经放出固件更新修复了后门问题，并对 SEC Consult 表示感谢。 |
| 链接地址 | http://www.theRegister.co.uk/2016/12/06/sony_ip_camera_backdoor |

# 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 | 名称与发现时间 | 相关描述 |
|---|---|---|---|
| 移动恶意代码 | 新出现的样本家族 | RiskWare/Android.adplugin.a[exp]2016-12-05 | 该应用为一款广告插件，运行后，通过点击触发。在通知栏推送广告的同时会将用户的手机固件信息等上传至个人云网站，造成用户资费消耗和隐私泄漏。建议卸载。( 威胁等级低 ) |
| | | PornWare/Android.App4Porn.a[rog]2016-12-07 | 该类应用为色情播放器程序，包含色情敏感内容。建议使用健康绿色软件。( 威胁等级低 ) |
| | | Trojan/Android.MFSocket.a[prv，spy]2016-12-08 | 该应用运行后会获取 Root 权限，释放资源文件 adbDownload；会联网并通过 Socket 通信，根据获取到的指令，上传用户的短信、GPS、图片、语音视频、固件信息、通讯录和通话记录等隐私信息，同时检测是否包含暴恐相关信息。( 威胁等级中 ) |
| | 较为活跃的样本 | Trojan/Android.Dropper.d[exp，rog] | 该应用包含危险行为代码，会私自下载安装软件，造成用户流量等资费消耗。( 威胁等级高 ) |
| | | G-Ware/Android.HiddenAds.an[rog，exp] | 该应用会伪装成 Facebook 应用，运行后会隐藏图标，后台加载弹窗广告，造成用户资费损耗。建议立即卸载。( 威胁等级低 ) |
| | | Trojan/Android.FakeApp.cf[exp] | 该程序会伪装成 Whypay 应用，运行后会隐藏自身图标，并请求系统辅助功能。如申请不被通过则会不断弹出置顶窗口持续申请，影响用户正常使用。同时，静默下载安装正常的 Whypay，静默下载安装未知应用的代码，造成用户资费消耗。建议卸载。( 威胁等级中 ) |
| | | Trojan/Android.Downloader.cr[exp，rog] | 该程序会伪装成正常软件，安装后无图标显示，会静默下载并安装软件。存在隐私泄露，流量消耗等安全隐患。建议用户卸载。( 威胁等级中 ) |
| | | Trojan/Android.Rootnik.m[rog，sys] | 该应用会伪装成正常应用，运行后会获取 Root 权限，下载并静默安装应用，静默卸载应用，造成用户资费损耗和系统稳定。建议卸载。( 威胁等级高 ) |
| PC 平台恶意代码 | 活跃的格式文档漏洞、0day 漏洞 | Apache Tomcat 多版本远程代码执行 (CVE-2016-8735) | Tomcat 是运行在 Apache 上的应用服务器，支持运行 Servlet/JSP 应用程序的容器——Tomcat 可看作是 Apache 的扩展，不过实际上 Tomcat 也可以独立于 Apache 运行。Oracle 修复了 JmxRemoteLifecycleListener 反序列化漏洞 (CVE-2016-3427)。Tomcat 中也使用了 JmxRemoteLifecycleListener 这个监听器，但是 Tomcat 并没有及时升级，所以导致这个远程代码执行漏洞。( 威胁等级高 ) |
| | 较为活跃的样本 | Trojan[Ransom]/MSIL.Vulnsym | 此威胁是一类勒索型木马的解密程序。该家族样本运行后为一个对话框形式的解密程序，需要填入指定的密钥，应为某种勒索型木马的解密程序。( 威胁等级中 ) |
| | | Trojan/Win32.Recslurp | 此威胁是一种下载恶意代码并运行的木马家族。该家族样本运行后，会复制自身到三个系统的关键位置并分别命名为 Csrss.exe、Rundll.exe、Svchost.exe，运行后可以改变系统防火墙策略，连接远程服务器下载等，有一定风险。( 威胁等级中 ) |
| | | Trojan[Downloader]/JS.Cryptoload | 此威胁是一种下载恶意代码的木马家族。该家族样本是 JavaScript 脚本，包含下载恶意代码的 URL，其他脚本可以对其进行调用，下载后可以加密用户文件的恶意代码。( 威胁等级中 ) |
| | | Trojan[Backdoor]/Win32.Thunkan | 此威胁是一种后门程序。该家族样本使用了简单的加壳手段来隐藏自身的关键字符串，运行后会建立后门，可以从远程服务器下载其他恶意代码并运行，有一定威胁。( 威胁等级高 ) |

# IBM “沃森”打击网络犯罪

Brian Barrett / 文　安天公益翻译小组 / 译

“沃森”(Watson) 是 IBM 研发的全才型超级计算机，在编写食谱、设计服装、预测天气等领域都有突出的表现。现在它正面临着最大的挑战：预防金融、医疗保健和其他领域的网络犯罪。

从今天开始，40 家企业将依靠沃森计算机的认知能力来打击网络犯罪活动。沃森所积累的现实生活经验将帮助它磨练技能和在特定行业中工作，因此“沃森网络安全”测试计划对 IBM 也有益处。沃森的网络安全技能并非从零开始，IBM 研究人员从去年春天开始培训它网络安全基础知识，以便它可以分析和预测威胁。经过培训后，沃森开始投入到现实生活中，进一步的磨练技能，可以将其视为世界上最聪明的实习生。

近期，沃森计算机做了很多功课。网络空间是庞大的，沃森认识和理解的越多，越能有效的区分良性威胁和恶意威胁。沃森最重要的能力不是大量的处理信息，而是通过将结构化数据 ( 如特定安全事件 ) 与非结构化数据 ( 如白皮书、研究报告 ) 相结合，从而将信息综合处理。

Forrester Research 分析师 Andras Cser 说：“认知计算比传统的基于规则的系统快 30-40%。”他补充说，像沃森这样的认知系统会减少误报。通过不断学习，它不会再犯同样的错误。

不过在此之前，沃森需要进行学习。研究人员每月向沃森提供 15,000 份文档 ( 将其链接到数据库 ) 和实时新闻，以保持数据库的更新。数据积累只是其学习的一部分，沃森必须明白词语的意思，才能知道它们之间的关系。

以“勒索软件”为例，勒索软件是一种日益普遍的黑客攻击，它会挟持被攻击者的计算机和操作系统，迫使受害者支付赎金。初期，沃森以为“勒索软件”是一个地名。IBM 副总裁 Caleb Barlow 说：“我们猜测，沃森认为‘勒索’是几个城市的名称，‘勒索软件’不是大多数字典中通常出现的意思。沃森在积累的数据中找出该词的意思，将它断定为一个位置。”

当 IBM 研究人员在“勒索软件”文档中给出定义时，沃森终于明白这跟城市无甚关系。通过这个有趣的例子也说明了沃森所面临的挑战和机会。遇到不明白的内容，它可以根据上下文进行推断。如果判断错了，便以此积累经验。一旦它学会了，就不会忘记，这也是测试计划的出发点。

现在，沃森的测试也不像传统软件的测试那样。

Barlow 说：“在常规开发项目中，我们分配一个测试矩阵进行测试，以了解软件在测试中的表现。对于沃森的情况，更像是人类的学习。在小学、高中、大学和工作后，不同的阶段要积累不同的知识以及经验。沃森的知识储备历程与之类似。”

换句话说，沃森目前了解了安全行业的基本知识。接下来，它必须学习出现在各种使用案例中的特定术语。“医疗保健行业的安全语言会不同于能源行业的安全语言。”Barlow 说。

在测试期间，沃森将与几十家公司合作，向其安全分析人员提供报告和建议。具体来说，沃森可以识别安全事件是否与已知恶意软件相关，并提供相关背景，识别可疑的用户行为。( 以密码输入为例，重复失败的密码输入是因为用户忘记密码，还是入侵企图？ )

沃森不会取代人类，而是帮助他们更快、更全面地响应。IBM 的研究表明，安全团队每天平均扫描 20 万个潜在重大安全事件，利用计算机处理这些安全事件能够节省大量的时间。

Avnet的安全主管 Sean Valcamp 表示，“我将传统的网络安全分析模型，比作站在高速公路旁的交警，试图找出潜在的违法者。车辆在路上高速行驶，很难确定谁超速了，谁开的是偷来的车。使用沃森，就像乘着直升机检查同样的高速公路。”

沃森并不能 100% 的准确，这就是测试的目的所在。它会在犯错的过程中学习，并捕获一些人类不意察觉的事件。在此过程中，沃森能够保护公司及其客户免受潜在的严重威胁。对于不久之前还在地图上寻找“勒索软件”的沃森来说，这个学习进步很大。

| 原文名称 | IBM's Watson Now Fights Cybercrime in the Real World |
| --- | --- |
| 作者简介 | Brian Barrett，《连线杂志》的编辑。 |
| 原文信息 | 2016 年 12 月 6 日发布于《连线杂志》，原文地址 https://www.wired.com/2016/12/ibm-watson-for-cybersecurity-beta/ |
| 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《Bitter 远控家族分析报告》

近日，安天追影小组在整理网络安全事件时，针对 Windows 平台下名为“Bitter”的木马家族进行了简要的分析。该家族木马的网络通信数据包通常包含“BITTER1234”字符串，故命名为“Bitter”家族。攻击者会给目标发送伪装好的 DOC 和 XLS 文档，而这些文档含有或能被利用下载 RAT 的恶意代码，并采用 CVE-2012-0158 漏洞进行伪装，试图在被感染的系统中盗取敏感文档。

安天追影小组针对 Bitter 木马家族的样本进行分析，发现该样本使用 Microsoft Visual C++8.0 进行编译，Bitter 家族旧变种是通过未加密的 HTTP POST 传递 C&C 信息，而在该样本中采用的是加密的 TCP 连接。样本程序试图将自身伪装成 Microsoft Printer Spooling Service，并带有不受信任的数字签名。此外，样本还会调用 CMD Copy 命令，将自身复制到系统“\Application Data\”目录并重命名，通过创建多个线程来与 C&C 建立连接并循环接收消息，执行命令。

经分析，该 RAT 样本包含以下几种功能：获取系统信息（计算机名称、用户名称、操作系统版本）、枚举逻辑驱动器、枚举日志文件以及它们的时间戳、打开远程命令 Shell、列举活跃的 UDP 连接、控制正在运行的进程、文件下载。利用这些功能，攻击者可以远程控制受害者的电脑。Bitter 家族使用免费的 DDNS 服务，建立自己 C&C 托管服务器，并使用 Gmail 伪造自己的身份信息。

该样本在被感染的设备上识别了逻辑驱动器后，会进行枚举文件，并检查它们是否匹配硬编码在样本中的文件扩展名为 DOC、PPT、XLS、DOCX、PPTX、XLSX、PDF、ZIP、7Z、TXT、RTF 等。因此可以判定，该样本的目的是窃取这些扩展名类型的敏感文件。

随着对 Bitter 家族的分析，可以发现越来越多的恶意代码使用公共网络服务来设置自己的 C&C，例如，免费的 DDNS 服务、Gmail 等，这使得防御和治理的难度有所提高。安天提醒广大网络使用者，要提高网络安全意识，收发邮件时要确认收发来源是否可靠，不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施。

## 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、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、数字证书鉴定器、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。

最终依据动态行为鉴定器将文件判定为木马程序。

该文件具有以下行为：感染文件、连接网络、自启动、获取驱动器类型、增加 run 自启动项、结束进程、遍历进程。

| | |
|---|---|
| 文件名 | B89E1CB807779F405C5B7CD122880E2E |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 321 KB |
| MD5 | B89E1CB807779F405C5B7CD122880E2E |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan[RAT]/Win32.Bitter.a |
| 判定依据 | 动态行为 |

◆ 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，Office 2007，Flash，WPS，FoxitReader，Adobe Reader |

◆ 其他行为

| 行为描述 | 危险等级 | 行为描述 | 危险等级 |
|---|---|---|---|
| 感染文件 | ★★ | 连接网络 | ★ |
| 自启动 | ★ | 获取驱动器类型 | ★ |
| 结束进程 | ★★ | 增加 run 自启动项 | ★ |
| 遍历进程 | ★ | | |

◆ 文件操作

| | |
|---|---|
| 操作 | 新建 |
| 文件路径 | c:\windows\system32\cmd.exe |

报告地址：https://antiy.pta.center/_lk/details.html?hash=B89E1CB807779F405C5B7CD122880E2E