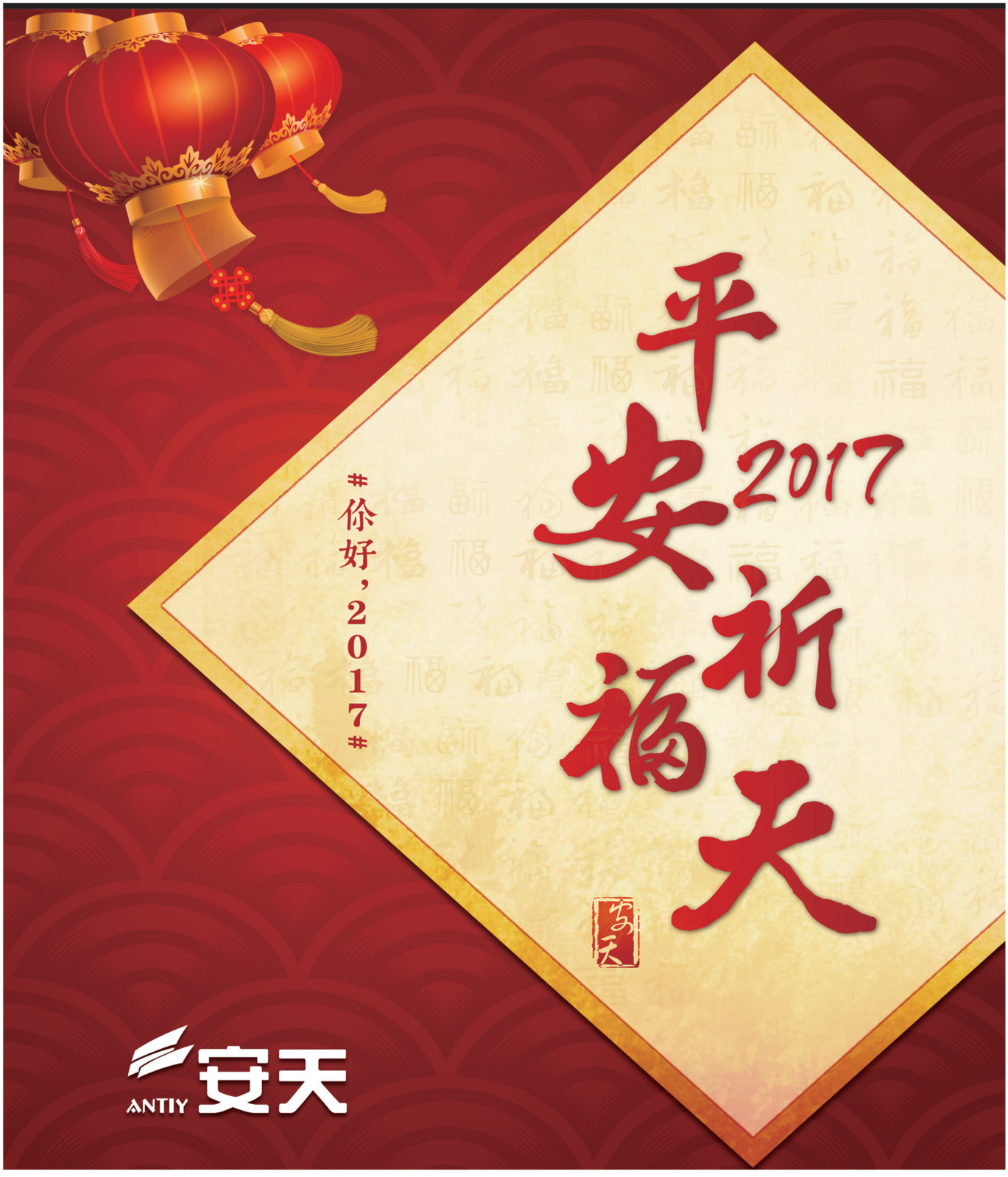
安天周观察

主办：安天　　2017 年 1 月 3 日（总第 71 期）试行　本期 4 版　　微信搜索：antiylab　　内部资料 免费交流



2017 年 1 月 3 日（总第 71 期 试行）
邮箱：antiynews@antiy.cn

新故相推，日生不滞，开启新一年的方式是自我梳理。

2016，安天的小图文志

艰难摸索

2016 年初，安天举办了营语为“朔雪飞扬”的第三届网络安全冬训营，在开营仪式上发布了《2015 威胁年报》的预发布稿。供应链遭遇攻击导致的防御正面不收敛、商业军火导致的高级攻击门槛下降、黑产大数据导致的威胁情报反用、以及线上线下结合的复合攻击方式成为新威胁的发展趋势，给网络安全带来了巨大的压力和挑战。

而特别让我们深入思考的是，高级攻击者普遍搭建模拟沙盘，对防御方各种安全产品进行模拟测试。如何让安全产品在客户侧形成攻击者难以预测的能力？在经过了不断的尝试、思考和对抗演练后，安天确定了以“下一代威胁检测引擎、深度客户赋能、知识化支撑和交互式可视化分析”为导向建立安天产品基因。

2016 年，安天先后发布了全新版本的终端防护产品“智甲”、流量监测产品“探海”、深度分析产品“追影”、威胁情报产品“AVL insight”等，对产品线进行了完善改造，并以“下一代威胁检测引擎、深度客户赋能、知识化支撑和交互式可视化分析”为导向建立安天产品基因。安天也成功树立了在军队、公安、海关、电力、金融、运营商等高安全等级客户的标杆案例，并承担了多个态势感知与监控预警平台的总体研发工作。

面对威胁情报这一新兴热点，安天不盲从潮流，坚持以可靠检测分析能力支撑威胁情报。从 AVL Inside 到 AVL Insight，安天全力挖掘检测引擎卡位特色和能力优势，使之达成更有效的用户价值。AVL Insight 是国内首个移动威胁情报平台，通过对移动威胁的全面感知和快速分析响应，多维度呈现高价值、定制化情报信息，并提供移动威胁的预警和处置策略。该平台旨在提高银行、政府等大型机构对威胁事件的感知、预警、预防、取证、响应和处置能力，以达到降低 IT 安全成本，提高资产和信息安全保障的最终目的。

这一版本的智甲、探海、追影等在安天内部遭遇了深入的反思和批判，没有这种自我否定和审视安天就很难进步。

安天 CERT 定期与产品研发部门进行“红蓝对抗”，在敲诈者病毒防御上，“红军”取得了 2015 年的首胜。这也是“红军”历史上第一次战胜“蓝军”。

本着赋能伙伴与客户的思路，安天继续推动反病毒引擎的生态协作，全球内置安天反病毒引擎的手机已经累计超过 5 亿部，防火墙和其他安全设备已经超过 10 万台。

刀锋战斗

2016 年，安天持续跟踪分析数十个 APT 组织的行动线索。并对两起重大 APT 事件成功实现了前期储备，适时曝光。并编写了有关移动恶意代码、敲诈者病毒、ATM 木马等内部和公开分析报告近百篇。

从 2016 年 1 月 5 日，安天与四方继保和复旦大学成立联合分析小组，展开对乌克兰停电事件分析，到 2 月 24 日《乌克兰电力系统遭受攻击事件综合分析报告》发布，其中经历了两个月。分析小组内大家反复争论研讨，报告几易其稿。报告指出：这是一起以电力基础设施为目标；以 BlackEnergy 等相关恶意代码为主要攻击工具，通过 BOTNET 体系进行前期的资料采集和环境预置；以邮件发送恶意代码载荷为最终攻击的直接突破入口，通过远程控制 SCADA 节点下达指令为断电手段；以摧毁破坏 SCADA 系统实现迟滞恢复和状态致盲；以 DDoS 服务电话作为干扰，最后达成长时间停电并制造整个社会混乱的具有信息战水准的网络攻击事件。这份报告也被国家有关能源安全专家称为国内外对此事件最好的一份报告。

2016 年 7 月 10 日，安天公布了 APT 分析报告《白象的舞步——来自南亚次大陆的网络攻击》，对南亚次大陆某国对中国的网络攻击进行系统曝光。除了样本分析外，安天基于代码工程规模和公开数据分析了攻击团队的规模，进行了人员画像。在报告中安天人沉重的写下了这样的话“大国防御力，由设计所引导、以产业为基础、与投入相辅相成，但最终其真实水平，要在与攻击者和窥探者的真实对垒中来检验。”

2016 年 11 月 4 日，安天发布了《从方程式到方程组——EQUATION 攻击组织高级恶意代码的全平台能力解析》，首次公布安天对方程式攻击组织针对 Solaris 平台和 Linux 平台的部分样本分析，安天分析团队自豪的说，“这是业内首次正式证实这些‘恶灵’真实存在的公开分析”，这篇报告以中英文双语发布，在海内外都引发了回音。

安天威胁情报系统，在事件分析中开始显示威力，安天 AVL Team 在 2016 年 4 月 28 日发布了重要分析报告《针对移动银行和支付交易系统的持续黑产行动披露》。

而在 Mirai 事件后，安天快速推出分析报告《IoT 僵尸网络严重威胁网络基础设施安全》，并认为不能单纯的用 DNS 安全的视角看待事件，“但 IoT 僵尸网络绝不仅仅是这起攻击事件的道具”，“被入侵的这些设备本身具有更多的资源纵深价值，这比使用这些设备参与 DDoS 攻击所带来的危险更为严重。其大面积的脆弱性存在，有着更为隐蔽、危害更大的社会安全风险和国家安全风险。只是这种风险，更不容易被感知到罢了。”

使命担当

2016 年“419 座谈会”向习近平总书记汇报后，安天创始人、首席技术架构师肖新光告诫团队：“这次我作为发言代表，不是因为安天做出了什么成绩，而是面对网络安全领域很多艰巨的困难、挑战和亟待解决的问题，业内群策群力讨论形成意见建言，我有幸作为代表将这些内容向总书记汇报。因此我们没有任何可以骄傲自满的理由。我们需要加快努力。期待有一天我们有向总书记进行工作汇报的机会”。

2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，在黑龙江省委书记王宪魁、省长陆昊、哈尔滨市委书记陈海波、市长宋希斌的陪同下，视察了安天哈尔滨总部。

在听取了汇报后，总书记对安天人说，“你们也是国家队，虽然你们是民营企业”。这是对安天坚持产业报国理想、坚持自主研发创新、坚持创造客户价值、坚持在网络强国中承担责任的鼓励。但这句话更是责任与期待，“国家队”三个字，使命何其重大！责任何其沉重！安天只能加倍努力，方能不辜负期许。

团队面容

安天的 2016，很多记忆定格在那些照片中，那些熟悉的面孔，那些新鲜的面孔，微笑，充满坚定，充满期待。

◆ 李柏松是每天早上分享“安天安全简讯”的那个人，是习近平总书记视察安天时，与之亲切交流的那个人，也是安天副总工程师。

◆ 一张自拍，安天员工用这样的方式记录总书记视察安天的瞬间。这是 90 后们的方式。她们是自拍狂人，她们也是安天的工程师。

◆ 安天各地举办 16 周年纪念活动，大家用最热情直接的方式表达对公司的祝福。

◆ 销售部，是安天最年轻的团队。2016 年安天销售体系形成建制，覆盖 5 大行业和全国 6 个片区。

本文内容转载，略有删节，文内所有分析报告可在安天网站及微信公众号 antiylab 查看。

旋律

我们唱响自己的歌，但我们不是网络空间的游吟歌者，我们是捍卫网络安全价值的工程师，我们是与威胁对抗的战士。

2016 年 12 月，傲气安天乐队举行了成立两年以来的第一次内部演唱会。其中包括原创招牌曲目“安天民谣三部曲”和安天校园招聘主题曲《我们在路上》。

一切伟大的事业，或始于江湖，终成于沧海。

2017，安天将继续变革、继续战斗！

安天发布《TeleBots 分析报告》

近日，安天追影小组在整理网络安全事件时，注意到一组恶意软件工具集，该工具集被称作 TeleBots。其操控者使用的工具集与曾经攻击乌克兰电网的 BalackEnergy 组织使用的恶意软件存在大量的相似处。他们都包含宏文档、下载器、后门、密码窃取器、键盘记录器、硬盘数据擦除器等，以此，可推测 BlackEnergy 组织已演变成为 TeleBots 组织。

黑客使用包含恶意宏的 Microsoft Excel 文档进行鱼叉式网络钓鱼攻击，以达到感染目标主机的目的。一旦受害者点击“启用内容”按钮，TeleBots 文档中的恶意宏会释放一个命名为 explorer.exe 的恶意二进制文件，并执行该文件。

追影小组针对 TeleBots 工具集中的后门程序进行了分析，发现该样本使用 Telegram Bot API，从而通过 Telegram Messenger 与攻击者进行联系。

另外，追影小组发现每一个样本都有一个独特的标记码嵌入在其代码中，即每一个样本都有它自己的 Telegram 账户。由于恶意样本通过私人的聊天软件进行通信，所以被感染的主机和攻击者之间的通信看起来就像是与一台合法服务器的 HTTP(S) 通信，且任意一台安装了 Telegram Messenger 的设备都可以作为 C&C 服务器。即便它只是一台智能手机，但它依旧能够通过聊天软件来发送 C&C 指令。Telegram Bot API 并不是该组织使用的唯一的合法协议，Outlook 邮箱也被该组织当做 C&C 服务器使用。

与其它的远控程序类似，TeleBots 的控制端可以通过指令控制受感染的机器，使其执行 Shell 指令并执行聊天返回、捕获屏幕、收集系统信息等操作。此外，恶意样本会自动同步控制服务器上指定目录的文件，进而对执行同步的文件进行感染。

随着对 TeleBots 家族的分析，追影小组发现攻击者利用 Telegram Bot API 而不是使用一台传统的服务器。由此可以发现网络罪犯者在不断的更新技术，不断的编写新的恶意软件。

网络安全是一场攻防博弈，安天会持续提高对恶意软件的检测能力，不断进行学习研究紧跟技术的步伐。

同时，安天提醒广大网络用户，要提高自身的安全意识，对于来源不明的邮件，不要轻易点击或者复制邮件中的网址，更不要轻易下载附件，以防止钓鱼邮件中的恶意代码的感染。

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、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：遍历进程、读取自身文件、获取计算机名称、释放 PE 文件、获取系统内存、打开自身进程文件、连接网络。

文件名	75EE947E31A40AB4B5CDE9F4A767310B
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	5.02 MB
MD5	75EE947E31A40AB4B5CDE9F4A767310B
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.TeleBot.A
判定依据	动态行为

报告地址：https://antiy.pta.center/_lk/details.html?hash=75ee947e31a40ab4b5cde9f4a767310b

◆ 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
遍历进程	★	读取自身文件	★★
获取计算机名称	★	释放 PE 文件	★
获取系统内存	★★	打开自身进程文件	★
连接网络	★		