安天周观察

主办：安天　2015 年 11 月 23 日 (总第 17 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加 2015 XDef 安全峰会并演讲

11 月 19 日 –20 日，武汉大学空天信息安全与可信计算教育部重点实验室主办的第四届全国网络与信息安全防护峰会 (XDef 安全峰会) 在湖北武汉举行。来自政府相关部门、全国各大高校、相关企业、科研院所以及民间安全团体的近 300 名专家学者参加了本次峰会。

安天移动安全研发中心总工程师乔伟发表了题为《面向威胁的移动反病毒工程化体系思

考》的技术报告。主要介绍了从反恶意代码领域看到的威胁现状，并重新审视了恶意代码检测的挑战和责任——既要坚持数据驱动，以体系化策略应对恶意代码的整体威胁，也要开拓思路，从情报驱动，有针对性的对恶意代码背后的威胁进行深入分析和应对。通过对安天在移动反恶意代码中使用的数据解析、脱壳的关键技术等描述，为大家呈现了针对恶意代码威胁的立体防御和检测体系构架。他说道：我们得到的最大反思不是我们检出了多少恶意代码，而是不忘初心，持续应对和挖掘恶意代码背后的威胁挑战，进行持续和有效的打击。

安天实况转播亚冠　助威恒大夺冠

11 月 21 日 20 点，2015 亚冠决赛广州恒大主场迎战迪拜阿赫利。安天哈尔滨及北京公司实况转播了该场比赛，并为前来观战的员工准备了丰富的零食及酒水，

激烈精彩的比赛使得欢呼声此起彼伏。最终广州恒大以 1:0 赢得比赛，夺取亚冠冠军，再次用实力证明了自己。

会议速递

◆ FSI2015 暨第八届中国互联网安全研讨会 (ISF) 召开在即

第八届中国互联网安全研讨会 (ISF) 将于 11 月 26 日至 27 日在上海召开，主题为“新互联网金融安全”，由 CISRG 主办，安天实验室和 AVL 反病毒引擎开放平台协办。今年的研讨会将由 ISF 跃升为 FSI，从互联网安全论坛 (Internet Security Forum) 成为了安全创新之未来 (Future of Security Innovation)。会议期间，安天代表马志远将发表题为《基于威胁情报的企业安全价值观》的演讲，同与会专家分享工作经验。

◆第三届安天网络安全冬训营即将启幕

第三届安天网络安全冬训营“朔雪飞扬”将于 2016 年 1 月 7 日至 9 日在哈尔滨友谊宫举行。本届冬训营将以“情报的支撑，塔防的实践”为核心议题，课程涵盖塔防模型的修订与实践、ARK 工具与主机系统安全、APT 事件分析等内容。安天将延续前两届冬训营的初衷，为网络安全保卫者与爱好者们提供一个分享、交流的良好机会与平台。

安天获“2014 年度江苏省网络安全信息通报优秀成员单位”表彰

11 月 17 日，由江苏省网信办、江苏省通信管理局指导，江苏省互联网协会主办的“第三届江苏省互联网大会”在南京召开，以“网联你我，安全护航”为主题的网络安全分会也同期举行。

在网络安全分会上，国家计算机网络应急技术处理协调中心江苏分中心，分别授予安天、中国电信股份有限公司江苏分公司、北京奇虎科技有限公司、亚信科技 (成都) 有限公司为 2014 年度江苏省网络安全信息通报优秀成员单位，以肯定各单位对江苏网络安全做出的贡献。在 2014 年，安天在南京青奥会、首届“国家公祭日”等重大保障中，提供了安全协助与配合；同时，在网络安全信息收集工作中，报送了大量有利信息，起到了净化江苏省网络环境的积极作用。

Chrome 浏览器 0day 使得数百万安卓设备遭受远程威胁

目前，黑客可以使用一种全新的方式来攻击安卓智能手机。通过利用代码使用 JavaScript V8 引擎中的一个漏洞，该引擎预装在几乎所有版本的安卓手机中，攻击者只需诱使潜在受害者访问一个包含有针对 Chrome 浏览器的恶意利用代码的网站。一旦受害者访问了这个网站，在无需与用户进行任何交互的情况下，恶意程序就可以安装任何恶意应用，使黑客能够远程获取手机的完整控制权。(文章来源：http://securityaffairs.co/wordpress/41967/hacking/android-chrome-exploit.html)

每周安全事件

类 型	内 容
中文标题	因在 CTF 比赛违规，巴西陆军遭报复导致数据泄露
英文标题	Cyberwar games lead to foul play resulting in leaked Brazilian Army data
作者及单位	Carolina，HackRead
内容概述	近日，巴西陆军的服务器被攻击，导致大约 7000 军事官员的个人资料被盗。黑客迅速公布了这些私密数据，其中包括国家保险号码和用于访问官方军事网站的 ID 和密码以及其他的一些详细资料。 这次攻击是一次报复，因为之前巴西军队曾参加 CTF 网络安全竞赛，并赢得比赛。但黑客称，巴西陆军团队曾通过 WiFideauth 赢得比赛，而这是禁用的技术。他们的这次攻击行动是为了表示抗议。
链接地址	http://www.hackread.com/brazilian-military-server-hacked/

每周值得关注的恶意代码信息

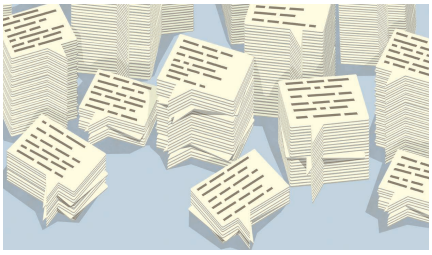
经安天检测分析，本周 7 个移动平台和 7 个 PC 平台的恶意代码家族值得关注

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	G-Ware/Android.E4Asms.j[prv] 2015.11.16	该应用程序安装之后无实际功能，可在后台监听收件箱，上传收件箱内容到指定服务器，造成用户隐私的泄露。(威胁等级中)
		Trojan/Android.emial.cf[prv，rmt] 2015.11.17	该应用伪装“最高人民检察院”，监听广播私自启动，上传用户手机号码、定位信息、联系人信息和收件箱短信，同时拦截短信向从服务器获取的手机号码转发，建议用户立即卸载，以免造成更多损失。(威胁等级中)
		Trojan/Android.lazyor.b[prv，exp] 2015.11.18	该应用程序运行后释放子程序，隐藏自身，伪装成系统应用，自身会联网获取指令，向指定号码发送指定短信，释放子程序应用会打开色情页面，无实际意义，对用户的安全造成极大损害，建议用户立即卸载。(威胁等级中)
		Tool/Android.SMSBomber.s[exp] 2015.11.19	该应用程序是一款短信炸弹工具，点击之后会向指定号码发送大量短信，会造成资费消耗，建议谨慎使用。(威胁等级中)
	较为活跃的样本	Trojan/Android.SmsThief.z[prv] [prv]	该应用程序伪装成其他软件，安装运行之后窃取用户短信收件箱详细数据联网上传，并删除指定短信，拦截短信，造成用户隐私泄露。(威胁等级中)
		Trojan/Android.SmsZombie.h[prv]	该应用程序运行诱导用户安装恶意子包，恶意子包会窃取用户账号密码，可能会窃取支付信息等用户隐私上传，建议立即卸载。(威胁等级中)
		Trojan/Android.wsms.b[prv，exp]	该应用运行后隐藏图标，拦截用户所有短信并通过服务器上传，对用户隐私造成严重损害，建议用户立即卸载。(威胁等级高)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office CVE-2015-2424 特制文件内存破坏漏洞 (MS15-070)	Microsoft Office 不正确处理特制的文件，存在内存破坏漏洞，允许攻击者构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。(威胁等级中)
	较为活跃样本	Trojan[Backdoor]/Win32.Agent.gen (详见第四版分析)	此威胁是一种木马类后门程序，运行后添加启动项，以达到随机启动的目的。具有远程桌面、键盘记录、开启摄像头等功能，是 Gh0st 类远控后门种变。(威胁等级中)
		Trojan[Downloader]/Win32.PassAlert.aec	此威胁是一种具有下载行为的恶意木马类程序。它通过电子邮件附件和不安全的网站链接传播。它可以伪装成常规文件来躲过杀软检查。它会通过漏洞来下载一些间谍软件和广告软件。(威胁等级中)
		Trojan[Backdoor]/Win32.PowerSpider.aep	此威胁是一种木马类后门程序，运行后可能会获取系统信息，主要目的是窃取用户在线游戏密码，并将窃取到的密码利用后门发送给攻击者。(威胁等级中)
		GrayWare[AdWare]/Win32.Lollipop.pu	此威胁是一种灰色软件类程序。在用户浏览网页时弹出广告，还可以重定向搜索引擎搜索结果，监测用户行为，下载其它应该程序，可能会发送用户信息给攻击者。(威胁等级低)
		Trojan[Downloader]/Win32.Banload.iu	此威胁是一种木马类程序，病毒运行后，复制自身到 %system32%\csrss\ 下，连接网络下载病毒文件，修改注册表，添加启动项，以达到随机启动的目的，该家族下载的文件可以盗取用户银行账号和密码，它是基于特定行为来命名的家族。(威胁等级中)
		Trojan[Dropper]/Win32.FrauDrop.rt	此威胁是一类伪装欺诈用户的黑客工具，通常对系统不具有任何危害。它通过警告信息等对用户进行欺骗，诱使用户购买其软件保护系统而使欺诈者获利，其出售的软件通常没有任何实际作用。(威胁等级低)

7000 万条囚犯通话录音被黑，律师 - 委托人特权形同虚设

Jordan Smith , Micah Lee / 文　　安天公益翻译小组 / 译

近日，一名黑客通过 SecureDrop 泄露了美国至少 37 个州的超过 7000 万条的囚犯通话录音。这些通话录音覆盖了从 2011 年 12 月到 2014 年春近两年半的时间。这名黑客认为美国监狱电话服务的领先供应商 Securus Technologies 侵犯了囚犯的宪法权利。



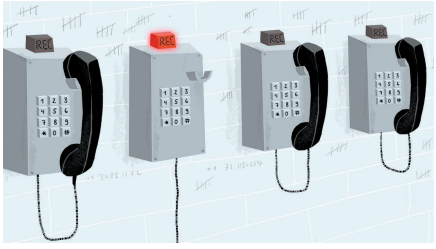
在这些录音中，囚犯和律师之间的通话至少有 14，000 条，有强烈迹象表明，至少有一些录音很可能是保密和授权的合法通信，它们根本就不应该被记录下来。因为记录受法律保护的律师 – 委托人的通信可能会触犯宪法，其中包括律师的有效援助权和与法院沟通权。

美国公民自由联盟的国家监狱项目总监大卫·法特希表示，“这可能是现代美国历史上最严重的律师 – 委托人特权侵犯事件，由于判决和监禁，很多囚犯的权利受到了限制，但是他们的律师 – 委托人特权仍然有效。”

Securus 是一家总部位于德克萨斯州达拉斯的电信公司，由一家私募股权公司拥有。其表面上的主要业务是为被监禁者提供电话和视频探访服务，为他们提供了一种与外面的亲人和律师保持联系的有效途径。

Securus 对政府客户自我推销，声称能够提供卓越的电话系统 Secure Call Platform，该系统允许广泛的监控和通话录音。同时，Securus 公司还推出了安全存储这些录音的能力，使它们只能被刑事司法系统内的授权用户访问。因此，Securus 的承诺不仅在于其巨大的数据库，还包括严格的安全标准。“我们将提供技术最先进的音频和视频通信平台，允许较高安全级别的通话。”该公司承诺道，“我们了解，通话的保密性是至关重要的。在商业活动中，我们将遵循所有联邦、州和地方法律。”

但事实上，Securus 存在重大的安全漏洞，黑客因此获得超过 7000 万条囚犯通话录音。被泄露的数据库包含囚犯的名字和姓氏，呼叫的电话号码，通话的日期、时间和持续时间，犯人的 Securus 帐号，以及其他信息。除了元数据，每个通话录音还包括“录音 URL”，可以下载通话的录音。



绝大部分被泄露的通话似乎是个人性质的，例如一对夫妇讨论《与星共舞》、电视晚餐、平时的通话费用 vs 食物费用。但被下载的音频文件引出了一个更大的录音数据库，录音的一个子集 (最少是 14，000 条) 是囚犯呼叫律师，通话时长从一分钟到超过一个小时。为了确定这一数字，《拦截者》查询了囚犯呼叫的近 130 万个电话号码中的每一个，与企业公共目录匹配，希望找出与该号码相关的律师事务所或律师办公室。

他们发现，Securus 记录了明显属于律师的至少 800 个号码的至少 14，000 条通话录音。但是，该数字很可能是被低估的，因为它不包括与律师手机号码的通话。换句话说，这 14，000 条通话可能只是遭到攻击的律师 – 委托人通话的冰山一角。总之，事实证明，Securus 也不怎么安全。

而且，这似乎并不是 Securus“据说坚不可摧的系统”第一次遭到攻击了。根据一位得克萨斯州律师提供给《拦截者》的文件，Securus 的系统在去年已经遭到了攻击。2014 年 7 月 18 日，有人入侵了囚犯阿隆·埃尔南德斯的 3 次通话，他是新英格兰爱国者队的前球员，因为杀害了一位朋友而等待审判。在 2014 年 7 月 21 日的电子邮件通信中，两名 Securus 员工讨论了这一攻击事件：他们发现，该系统被南达科他州的某人访问，但是他们不知道那个人的名字。“天哪 ..... 大事不好了。”其中的一封电子邮件说，“如果有人入侵了该系统，那么公司就麻烦了。”

没有迹象表明 2014 年的攻击事件被公开了，Securus 也没有就此做出任何回应。

原文名称	Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege
作者简介	Jordan Smith，Micah Lee，Jordan Smith 是一位居于德克萨斯州奥斯汀市的屡获殊荣的调查记者。
原文信息	2015 年 11 月 12 日《The Intercept》发布 原文地址 https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/
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 CERT 献译 OllyDbg2.01 版中文帮助手册

OllyDbg 作为一款结合 IDA 和 SoftICE 功能的调试工具，因其简易的操作和强大的功能，成为了安全研究领域使用最广泛的调试分析工具。目前 OllyDbg 软件已发布了 2.0x 版本，但内附的帮助手册尚无中文翻译版发布。基于合作分享，互利互惠的理念，为方便更多新版 OllyDbg 使用者，安天 CERT 对帮助手册展开了翻译工作，希望能够对广大 OllyDbg 使用者有所帮助。

OllyDbg2.01 是一款 32 位汇编级分析调试器，界面直观，在没有源代码或解决译别问题的时候，尤其适用。实际上，32 位调试器 OllyDbg 的第二版是经过推倒重来再设计的。因此，它将会比上一版本更快、更强、更稳定。2.01 版本具有一些 1.10 版本不曾拥有的新功能，主要包括：

1. 全面支持 SSE 和 AVX 指令集。SSE 寄存器可直接访问，无需经过代码注入。

2. 在调试器上下文执行命令时，可以跟踪执行速度——包括执行条件和记录——最高可支持每秒执行 1,000,000 条命令。

3. 内存断点数量不受限制。

4. 内存和硬件可设置条件断点。

5. 更为可靠，分析时不需要借助跟踪。

6. 分析器可识别未知函数的参数个数，有时还支持参数含义的识别。

7. 支持脱离 (Detaching) 被调试进程。

8. 支持子进程的调试。

9. 提供在 TLS 回调时暂停的选项。

10. 提供未处理异常过滤器，可放行未处理异常。

11. 内建整数和 FPU 命令帮助。

12. 可定制快捷键。

13. 用户界面支持多语言。

除了这些和 1.10 版本的区别外，OllyDbg2.01 还具有更多的特色功能，使其成为一款令人满意的调试器。这些功能在帮助手册中均有详细介绍，安天 CERT 将与安全研究领域的从业者分享中文版本的帮助手册，希望可以帮助各位使用者对 OllyDbg2.01 版本有更好地了解。(非官方译本的该手册已经整理为 PDF 版本，如有兴趣，请您联系安天人或发邮件至 antiynews@antiy.cn 索取。)

木马程序

第二版值得关注的【Trojan[Backdoor]/Win32.Agent.gen 威胁 (威胁等级中)】是一种木马类后门程序，运行后添加启动项，以达到随机启动的目的，具有远程桌面、键盘记录、开启摄像头等功能，是 Gh0st 类远控后门种变。

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、数字证书鉴定器、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 BD 静态分析鉴定器、动态行为鉴定器、智能学习鉴定器最终将文件判定为木马程序。

文件名	mmcpxwxvg_net.exe.zy
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	134 KB
MD5	013D52F050619524B6D15ADCD260C197
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.Agent.gen
判定依据	BD 静态分析

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
删除自身	★★★★	注册 tamper 服务	★★★★
服务 DLL	★★★	释放后缀为图片的 PE 文件	★★★

该文件具有以下行为：删除自身；注册 tamper 服务；服务 DLL；释放后缀为图片的 PE 文件；检查摄像头；获取 CPU 信息；释放 PE 文件；获取系统内存；获取计算机名称；访问 DNS；获取 socket 本地名称；创建服务；连接网络；获取驱动器类型；独占打开文件；遍历进程；从资源中释放 PE 文件；启动服务；查找指定内核模块。

同时，该文件通过 3 种方式对虚拟机、沙箱技术进行检测。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
检查摄像头	★★	获取 CPU 信息	★★
释放 PE 文件	★	获取系统内存	★★
获取计算机名称	★	访问 DNS	★
获取 socket 本地名称	★	创建服务	★
连接网络	★	获取驱动器类型	★
遍历进程	★	独占打开文件	★
启动服务	★	从资源中释放 PE 文件	★
查找指定内核模块	★		

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=013D52F050619524B6D15ADCD260C197