安天周观察

主办：安天　2015 年 12 月 14 日（总第 20 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加第十八届亚洲反病毒大会

近日，安天派出代表参加于越南举行的第十八届亚洲反病毒大会 (AVAR2015)。做为全球最顶级的反病毒研讨盛会，AVAR 大会堪称全球网络信息安全领域的风向标之一。本届会上，来自中国、德国、英国、日本、美国、澳大利亚等全球网络信息安全领域的数百位顶级专家齐聚一堂，共同探讨了全球网络案例新形势。

其中，来自 F-Secure 的 MikkoHypponen 进行了题为《保护我们的未来》的演讲，他指出用户在享受各种“免费”服务及软件的同时，个人的隐私内容也被这些公司获取。据统计，数十亿的个人隐私内容被非法利用，这其中包含以获取金钱为目的个人或团体，以及以监视和间谍为目的的政府行为。MikkoHypponen

安天代表在 AVAR 大会现场

在报告中还例举了一些具体事件，包括 spam 的全球分布情况、ransome 事件、加拿大提出的对车辆的安全评估，以及政府攻击事件 (Duke 家族) 等等。来自 ESET 的 Diego Perez 和 Pablo Atilio Ramos 讲述了 Liberpy 的发现过程。Liberpy 是一种基于 HTTP 的僵尸网络，它窃取用户信息并且可以通过 USB 设备传播。为了研究 Liberpy，ESET 做了 DNS 重定向到他们的 DNS“黑洞”服务，两位专家向与会嘉宾介绍了 Liberpy 的攻击手段及全球分布情况。

据了解，亚洲反病毒大会的组织者 AVAR(Association of Anti Virus Asia Researchers) 成立于 1998 年 6 月，是一个独立的、非盈利的、定位于亚太

安天受国家计算机病毒应急处理中心委托，向 AVAR 主席转交病毒应急中心的联络公函

地区的组织。其任务是预防由于恶意软件导致的破坏以及流行，同时在亚洲地区加强反病毒研究专家之间的交流与合作。

安天【CERT】发布

《一例以“采访”为社工手段的定向木马攻击分析》研究报告（见四版）

新型勒索活动会在数据加密之前盗取密码

新一波的秘密勒索软件开始攻击 Windows 用户。如果被袭击的用户的系统没有更新，一种名为 Angler 的开发工具会在常用的第三方软件和 Microsoft Windows 程序中扫描漏洞。一旦确认了安全漏洞，Angler 就会拓展他们并在受害系统中强行安装 CryptoWall4.0。

该工具最近一轮的攻击尤其恶劣，因为在加密之前，这种隐蔽式攻击使用了一种叫做 Pony 的恶意软件来截取任何储存在被感染电脑中的登录认证。对此，Windows 用户应该以最新的安全补丁更新运行系统、浏览器和插件，并且谨慎地卸载 Java 和 Flash。（文章来源：http://arstechnica.com/security/2015/12/newest-ransomware-pilfers-passwords-before-encrypting-gigabytes-of-data/）

安天系统分析工具 ATool 恢复更新

近日，安天系统分析工具 ATool 恢复更新，新增支持 Win7/8/10 32bit/64bit 系统，能有效发现隐藏在系统中的 Rootkit，同时支持对程序进行对照扫描（由 Virusbook 提供技术支持），可更好地全方位保护系统和个人信息安全。

ATool 最初于 2007 年发布，是一款反 Rootkit 工具，用于辅助杀毒软件对系统安全进行深度分析，能针对各类常见的主机问题及有害文件进行分析、诊断和处置，同时对系统的

共享及帐户等信息进行检查和修复。其特别提供的分析模块能够实现基于条件加权的未知木马检测，对系统中自启动项、任务、进程、服务、驱动、端口、SPI、插件、文件、注册表等内容进行严格地行为判断和特征分析，形成对每个文件的受信状态判定。ATool 曾在 2010 年暂停维护，此次恢复更新，安天意在为用户提供更好更高端的服务。用户可登录网址 http://tools.antiy.cn/dl/atool.zip 下载 ATool。

每周安全事件

类 型	内 容
中文标题	“Backstabbing”恶意软件通过受感染电脑窃取手机备份
英文标题	“Backstabbing”malware steals mobile backups via infected computers
作者及单位	ZeljkaZorz，HELP NET SECURITY
内容概述	近日，研究人员发现一些攻击者会从从受害者的电脑中窃取手机备份文件。他们将这种攻击技术称为“BackStab”，并称恶意攻击者和数据收集者一直在用 BackStab 恶意软件攻击世界各地，且持续多年。目前，这款恶意软件主要针对 iOS 用户，研究人员警告说：“在某些情况下，像 iTunes 这样的官方备份软件可能会为没有用户交互和加密的移动设备自动创建备份。此外，当设备被连接到一个受感染的电脑时，恶意软件也有可能会启动备份。”
链接地址	http://www.net-security.org/malware_news.php?id=3172

每周值得关注的恶意代码信息

经安天检测分析，本周 9 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.JSSMSers.a[exp，bkd] 2015-12-3	该应用伪装成食品、礼物、视频等程序，使用 droidgap 框架及 js 获取数据发送短信。并且会设置所有短信为已读状态，同时会拦截短信、拦截来电，此外部分应用会调用 youtube 程序播放视频。另外会上传手机型号等设备信息、并伴随有广告信息，给用户造成一定的资费损失。(威胁等级高)
		Trojan/Android.b4aspy.a[prv，spy，rmt] 2015-12-3	该应用为 b4a 语言编写的间谍应用，可通过远控指令控制用户手机，窃取用户短信、通话、拍照、浏览器浏览记录，下载其他应用并私自提权安装，对用户具有重要威胁，建议用户立即卸载。(威胁等级高)
		AdWare/Android.Magiccad.a[ads] 2015-12-4	该应用包含 AdLine 广告，运行后会以积分墙的方式推送广告，同时会获取固件信息和位置信息，可能会造成用户隐私泄露，建议谨慎使用。(威胁等级低)
		Trojan/Android.Koler.d[rog，fra，pay] 2015-12-5	该应用伪装成色情应用诱导用户点击，运行后激活设备管理器，隐藏图标，以非法浏览色情为由锁定用户界面，勒索用户付费；上传用户手机固件信息，私自拍摄照片，使用户无法正常使用。(威胁等级中)
	较为活跃的样本	Trojan/Android.emial.cl[prv，exp]	该应用安装无图标，运行后拦截转发短信、删除短信，获取收件箱并转发到联网获取的号码，造成用户隐私泄露，建议立即卸载。(威胁等级高)
		Trojan/Android.simplelock.k[prv，rmt，sys]	该应用伪装成色情软件，安装运行之后诱惑点击色情视频，接着弹出并置顶伪装的 FBI 勒索界面，并上传用户的通讯录、设备 IMEI、设备锁定状态。使用户不能正常使用设备以及隐私的泄露，建议不要安装该软件。(威胁等级高)
		Trojan/Android.emial.cm[prv，exp，fra]	该应用伪装成色情应用，运行后隐藏图标，后台拦截并转发短信，之后删除短信，造成用户隐私泄露，建议立即卸载。(威胁等级中)
		Trojan/Android.Downloader.ay[exp]	该应用安装无图标，触发启动，后台联网下载 Apk，静默安装，为了避免造成用户资费损耗建议卸载。(威胁等级中)
		G-Ware/Android.Fakegupdt.ah[prv，exp，rog]	该应用运行后隐藏图标，激活设备管理器，后台上传绑定邮件账号、安装列表等隐私信息，并创建桌面快捷方式推送应用，建议卸载，以避免造成隐私泄露和资费损耗。(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 未初始化内存使用漏洞 CVE-2015-1770	该漏洞可能在用户打开经特殊设计的 Microsoft Office 文件时允许远程执行代码。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。(威胁等级高)
	较为活跃样本	Trojan[PSW]/Win32.Tepfer.se	此威胁是一种木马类程序，可以在被感染的电脑上盗取用户账户信息 (用户名、密码)。它能通过垃圾邮件、可疑链接、恶意网站等侵入目标机器。它能通过下载不同的寄生网站、修改系统设置、更改或删除重要文件的方式感染计算机。(威胁等级中)
		Trojan/Win32.Qhost.ar	此威胁是一种木马类程序。改变 Host 文件内容以屏蔽某些网站的木马类程序。该家族能够通过专门用于改变 Host 文件的黑客服务器来重定向细节，从而实现对密码信息的窃取。(威胁等级中)
		Trojan[Downloader]/Win32.Small.qwe	此威胁是一种木马类程序，一般会伪装成正常文件欺骗用户下载或者通过一些恶意网页的辅助，通过浏览器和插件的漏洞被安装到用户的系统中。也有些变种由其他恶意软件释放或下载得到。(威胁等级中)
		Trojan[Downloader]/Win32.Zlob.ih	此威胁是一种木马类程序，感染用户系统之后，会修改系统设置，下载多种恶意软件并执行，对用户系统造成很大损害。(威胁等级中)

相互通信的汽车更易被窥探

Andy Greenberg/ 文　　安天公益翻译小组 / 译

将汽车彼此数字连接，并连接到公路基础设施上能够大大减少碰撞和交通拥堵现象。但是，无线车载通信是以你的隐私为代价的，从来不关闭通信的汽车可能更容易被追踪。

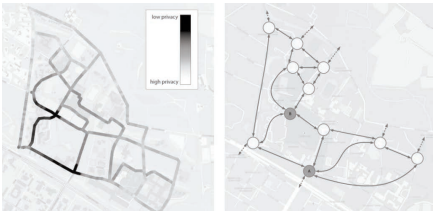
近期，荷兰特温特大学和德国乌尔姆大学的研究人员发现，他们可以使用几千美元的设备来追踪发射所谓的“连车”无线通信 (针对未来的车辆 – 车辆连接提出) 的汽车。将两个 550 美元的设备战略性地设置于特温特大学 432 英亩校园的路口处，研究人员就能够追踪汽车无线电通讯的独特特征，以 78% 的准确率预测汽车处于哪两个校园区域，以 40% 的准确率预测汽车在特定道路上的精确位置。从概念证明推断，研究人员认为，将相同的技术扩展到几十万美元的硬件上，政府、甚至业余爱好者就可以监控整个小城市的车辆。

国家高速公路交通安全管理局 (NHTSA) 将会考虑在 2017 年首次在美国强制实施连车协议，该协议使用类似 Wi-Fi 的 802.11p 无线信号，允许汽车相互通信，并与公路基础设施 (如公路或桥梁) 通信。2010 年的一项 NHTSA 研究估计，该协议可以防止多达 81% 的车辆碰撞。

但是特温特大学研究人员之一的佩蒂特表示，这种无线通信的范围大约介于 300 到 900 英尺，也可以作为一个强大的监控机制。目前还不清楚，连接车辆改变其独特的无线特征 (用于识别车辆) 的时间间隔，这种改变能够限制使用这些特征追踪个人的汽车。但是，鉴于这些“化名”长时间保持不变，佩蒂特认为连车协议可以提供相对廉价的车辆追踪方法，这可以加强现有的执法追踪技术，如自动读取车牌。或者，他想象，黑客可以从该系统中收集并获取数据，创建一个整个城市车辆移动的数据库。

“当你做这样的部署时，你需要考虑隐私问题。”佩蒂特说，“很明显，我们需要通过这种攻击来证明这些信息可以被任何人获得。”

在概念证明中，研究人员使用了两种 Cohda Wireless MK3 无线模块，将两个 Smarteq 天线彼此连接，总成本约为 1,100 美元。他们将这些模块置于特温特校园的两个路口，可以粗略地追踪载有活跃的 Nexcom 802.11p 无线电信标的车辆。下图显示了两个模块被放置的路口位置，“隐私图”展示了研究人员根据无线电读数预测汽车位置的准确率。



虽然，这两个模块只能以 40% 的准确率定位 65 英尺范围内的任何车辆的位置，但是研究人员推测，多几个模块可以提供更高的准确率。在路口上添加的每个无线模块都能够提供目标车辆的更多信息，如目标车辆的位置和方向。例如，如果研究人员覆盖校园 21 个路口的其中 8 个 (成本为 4,400 美元)，他们认为车辆位置预测的准确率可以达到 90%。

研究人员计算出，他们可以将该监控技术扩展到整个城市，而成本不足 50 万美元。他们写道，例如，该系统可以以约 36.2 万美元的成本覆盖附近的城市恩斯赫德 (该城市拥有超过 15 万人口和 3.52 万英亩土地)。他们认为，他们的“嗅探站”可以很容易地降低成本，他们甚至预测，可以很快地使用 Raspberry Pi 小型计算机以十分之一的成本创建这样一个“嗅探站”，从而极大地削减追踪成本。“如果你能够充分地覆盖一个城市，那你就可以追踪每一个人。”佩蒂特说。

佩蒂特指出，更频繁地为车辆编程并改变其独特的无线电特征可以减轻一些隐私问题。佩蒂特也承认，业界团体，如美国的防碰撞指标联盟和欧洲的车辆间通信联盟，正在考虑隐私保护问题。但是佩蒂特说，需要更多的研究来了解这些化名保护到底能够在多大程度上对抗追踪。研究人员警告说，如果设置足够高密度的追踪模块，攻击者甚至能够克服快速化名切换，从而无所不在地追踪车辆的下落。

“改变化名无法阻断追踪。它只能缓解这种攻击。”佩蒂特说，“但是，我们仍然需要用它来对抗中等规模的监控者 ..... 我们想要证明，在任何部署中，你还是得有这种保护，否则就会有人能够追踪你。”

原文名称	Cars That Talk to Each Other Are Much Easier to Spy On
作者简介	Andy Greenberg，《连线杂志》的资深作家，研究领域涵盖安全、隐私、信息自由和黑客文化。
原文信息	2015 年 10 月 27 日《连线杂志》发布 原文地址 http://www.wired.com/2015/10/cars-that-talk-to-each-other-are-much-easier-to-spy-on/
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】发布

《一例以“采访”为社工手段的定向木马攻击分析》研究报告

2015 年 12 月 2 日夜间，安天监控预警体系感知到如下信息线索：某知名作家在新浪微博发布消息，曝光有人以发送“采访提纲”为借口，利用微博私信功能，发送恶意代码链接。安天安全研究与应急处理中心 (安天 CERT) 根据微博截图指向的链接，下载该样本并连夜展开分析。

该恶意样本是一个自解压程序，使用了十多个加密脚本执行不同的恶意功能，最终目的是在用户系统中安装后门程序。经安天 CERT 分析，发现其有两个后门程序，并且这两个后门程序的本地行为完全一致，开启系统进程 svchost.exe，并注入其中。通过代码分析，发现两者的动态域名跳转地址都为 115.**.***.239，从而可以推断出这两个后门都是同一网络行为与功能。

同时，经过安天 CERT 研究人员对后门代码以及上线数据包格式的分析，可以判定这两个后门为同一远程控制生成器生成，该远程控制软件是灰鸽子源码修改的 RemoteABC 远程控制软件的某一版本。此远程控制软件具有文件管理、进程管理、服务管理、共享管理、插件管理、远程开启视频和语音等功能。

经分析，攻击者具有以下作业特点：

1) 借助微博仿冒身份。

2) 利用百度网盘向目标人群投送恶意代码。

3) 借助常被用于处置恶意代码的工具软件，绕过系统及安全工具提供的保护机制。

4) 利用已知安全工具软件的安全漏洞，破坏安全工具软件，使之失去保护效果。

根据上述作业特点，可得出以下启示：

1) 互联网公司有必要加强对用户身份仿冒的监测与治理。

2) 网盘提供厂商应加强对存储内容的安全性检查，避免被利用传播恶意代码。

3) 工具软件的开发者在开发一些可能绕过、破坏系统安全机制的功能时，应尽量加入明显的用户交互确认功能，以免被恶意利用。

4) 安全工具开发厂商在发现安全漏洞后，应及时发布升级补丁，并建议用户立即更新，以免漏洞被攻击者绕过，而给用户带来安全假象。

(报告原文：http://www.antiy.com/response/RemoteABC/RemoteABC.html#rd)

恶意程序

安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对上述恶意程序进行有效检测，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。

最终依据动态行为鉴定器将文件判定为恶意程序。

文件名	南方周末采访提纲 .exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	5.12 MB
MD5	EA878E08F10057B2477090C8017AF587
病毒类型	恶意程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	动态行为

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
可疑进程名称	★★★★	关闭 UAC	★★★

该文件具有以下行为：

可疑进程名称；关闭 UAC；创建特定窗体；请求加载驱动的权限；获取主机用户名称；获取计算机名称；释放 PE 文件；获取驱动器类型；获取系统内存；查找特定窗体；独占打开文件；打开自身进程文件。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
创建特定窗体	★	请求加载驱动的权限	★
查找特定窗体	★	获取主机用户名称	★
获取系统内存	★★	获取计算机名称	★
独占打开文件	★	释放 PE 文件	★
打开自身进程文件	★	获取驱动器类型	★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=EA878E08F10057B2477090C8017AF587