安天周观察

主办：安天　2016 年 6 月 6 日（总第 42 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天移动安全公司与中国泰尔实验室达成战略合作意向

近日，安天移动安全公司 (AVL Team) 与中国泰尔实验室在移动安全领域达成战略合作意向。双方将借助各自在移动安全与智能终端操作系统等领域的领先优势，共同为手机厂商提供更为便捷、优质、可靠的服务。

AVL Team 专注于移动反病毒领域，致力向合作伙伴提供最好的反病毒引擎和解决方案。作为国内优秀的反病毒引擎供应商，AVL Team 在 2014 年获得全球顶级测评机构 AV-Test 年度最佳保护奖，成为国内首家获得国际安全大奖的公司，目前已为全球超过 40 家企业和机构提供移动安全解决方案。

中国泰尔实验室是国家信息通信研究领域最重要的支撑单位和综合政策领域的主要依托单位，也是国家级信息通信产品检测实验室。其建立了以 ISO/IEC 17025 为标准的质量体系，并通过了中国合格评定国家认可委员会 (CNAS) 以及德国国家认可机构 (DakkS) 的能力认可；获得国家认监委的中国强制性认证检验机构和国家统一推行的电子信息产品污染控制自愿性认证检验机构授权；开展电信设备进网检验；作为第三方实验室，是中国质量认证中心、泰尔认证中心、鉴衡认证中心、中国环境标志认证中心等众多国内认证机构的签约实验室；同时也是美国的 FCC、欧盟的 CE、加拿大的 IC、日本的 JATE、埃及的 NTRA 等国际准入制度的授权（列表）实验室。

在刚刚过去的“2016 中国网络安全年会”上，安天移动安全公司 CEO 潘宣辰作出了题为《移动威胁情报体系支撑生态实践分享》的报告，报告指出：安全行业是一个技术壁垒相对较高，同时追逐技术竞争力和技术差异化的行业，安全业内要形成良好生态环境，并不是单纯的输入输出或形成上下的关系，而是需要很多方面的努力。良好生态环境的形成和建设，既需要生态中不同角色之间有相依相生的关系，也需要有机与合理的双向关系。而安天移动安全公司与中国泰尔实验室的结盟作为移动安全技术领导者与国内信息通信领域顶尖机构合作的范本，无疑为移动信息安全领域的互惠合作，乃至整个智能终端良好生态环境的塑造提供了一个经典的案例。

此次战略合作意向的达成是双方务实合作，有效落地的一个里程碑。双方将确切落实习总书记所说的“整体设计，加强合作，相互学习，相互切磋，联合攻关，互利共赢”，努力促进双方各领域业务部门在移动信息安全、智能终端生态环境维护等方面的合作与交流，提升框架协同层次和水平，提升创新能力，实现战略发展中新的跨越，携手为广大设备厂商提供更加优质的服务。

黑客兜售可攻击 Windows 所有版本的零日漏洞

据外媒报道，近日，一名黑客公然在网上叫卖可攻击 Windows 所有版本的零日漏洞，售价为 9 万美元。该价格在 5 月 23 日更新，此前，黑客的定价更高，为 9.5 万美元。另外，他还在网上上传了两段该零日漏洞攻击的演示视频。该名黑客表示，这个漏洞将只卖给一个人，买家将能获取漏洞的源代码、完整的演示视频、微软 Visual Studio 2005 项目文件以及未来的更新，支付方式为比特币。同时他特别强调，该漏洞可以在 Windows 所有版本下运行，也就是说，15 多亿名用户将受到威胁。

而来自 Trustwave 及其他网络信息安全公司的专家们认为，这个漏洞的威胁性其实被黑客夸大了，因为它并不能感染电脑，而只能升级访问，进而成为一个二阶漏洞，通常用于获取持久性的启动权限，不过他们相信最终会有人买下它。（文章来源：http://m.cnbeta.com/view/506641.htm）

一周简讯

- 新恐怖主义担忧：黑客使用 GPS jamming 技术影响开罗机场
- LG 智能手机被发现严重漏洞，攻击者可获取设备控制权
- Tumblr 6500 万用户信息泄露，黑客在暗网廉价出售泄露信息
- 我国安全研究人员公开全球 24 款反病毒软件存在的安全漏洞
- 安卓间谍软件伪装聊天应用，窃取沙特阿拉伯政府安全求职者信息
- 安全厂商曝光巴基斯坦 APT 组织对印度政府的攻击行动
- 以色列研究人员声称设计出“完美”的隐蔽数据泄露技术

（安天 CERT 搜集整理，详见：http://bbs.antiy.cn）

每周安全事件

类 型	内 容
中文标题	韩国空军官方网站遭受网络攻击
英文标题	South Korea Air Force website hit by cyberattack
作者及单位	India Ashok；International Business Times
内容概述	近日，韩国空军官方网站遭受了大规模的网络攻击，持续关闭长达两周。据了解，有人冒充国防采办计划管理局官员，向当地国防承包商发送了一些可能包含恶意软件的可疑邮件，进行了可盗取本地国防承包商登陆信任许可的网络钓鱼诈骗。韩国空军正深入调查这次攻击背后的原因，当局者也将调查是否有数据泄漏的可能性以及网络上是否已经有相应的数据泄漏地址。韩国政府也正在采取措施以维持其网络基础设施的安全性，防止政府背景的间谍和黑客盗取其机密信息。
链接地址	http://www.ibtimes.co.uk/south-korea-air-force-website-hit-by-cyberattack-north-korea-involvement-not-ruled-out-1562054

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 4 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.Ltby.a[pay] 2016-05-30	该应用无实际功能，运行后会私自发送付费服务短信、监听短信、拦截包含指定内容的短信并自动回复，造成用户资费消耗。（威胁等级中）
		Trojan/Android.E4Atelnote.a[prv] 2016-05-30	该应用运行后诱骗用户输入 qq 账号和密码信息后上传到指定网站，获取用户定位信息、短信信息、通讯录和通讯记录信息上传到指定网站，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.Igamo.a[prv] 2016-05-31	该程序运行后在后台收集用户设备信息、位置信息、邮件信息等隐私上传到远程服务器，建议立即卸载，避免造成隐私泄露。（威胁等级高）
		G-Ware/Android.Fcounter.a[exp，fra]2016-06-01	该应用伪装系统程序，运行后上传手机已安装程序信息，后续联网私自下载指定程序执行推广操作，造成用户资费消耗，存在一定的安全隐患，建议及时卸载。（威胁等级低）
		Trojan/Android.Spstore.a[pay，prv]2016-06-01	该应用程序运行后私自调用支付模块，联网获取支付相关信息发送订阅短信，监听短信状态，上传支付记录到远程服务器，建议用户立即卸载，避免造成资费损耗。（威胁等级中）
		Trojan/Android.WYVadio.a[pay，prv]2016-06-02	该应用伪装成蓝牙应用，运行后隐藏图标，激活设备管理器，获取手机号码和固件信息参数上传，并根据联网返回数据，发送付费短信，拦截屏蔽短信，造成用户资费损失，建议不要安装。（威胁等级中）
	较为活跃的样本	Trojan/Android.muytpp.a[prv，rog]	该应用运行后会隐藏图标，私自提权静默安装包含的 apk 应用，联网上传短信、通讯录、通讯记录、浏览器书签、gps 位置等信息，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.FakeFlashPlayer.l[exp，prv，rmt]	该应用程序伪装 Adobe Flash，通过网络远程控制，接收指令后进行发送短信、上传收件箱信息、拨打电话、访问钓鱼网站等恶意行为，建议立即卸载，避免造成资费损耗和隐私泄露。（威胁等级高）
		Trojan/Android.E4AQQspy.e[prv]	该应用包含刷赞、刷钻、刷留言、图书 vip 等功能，其中图书 vip 会明文上传用户输入的 qq 账号和密码信息，可能造成用户隐私泄露。（威胁等级中）
		G-Ware/Android.HiddenAds.q[rog，exp]	该应用伪装系统程序，安装无图标，运行后释放子包，私自下载推广程序，执行创建桌面图标推广操作，还存在风险代码，会造成用户资费消耗，建议及时卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	OpenSSL 的 CVE-2016-2107 漏洞	CVE-2016-2107 漏洞对于开源加密库的影响可以被用来进行中间人攻击。只要用于连接的是 AES CBC 密码和支持 AES NI 的服务器，那么攻击者就可以利用“ Padding Oracle 攻击”解密 HTTPS 通信。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Banload	此威胁是一种具有下载行为的木马类程序，样本运行后连接网络下载其他恶意代码并安装，有可能导致用户信息被窃取，有一定威胁。（威胁等级中）
		Trojan/Win32.FakeAV	此威胁是一种伪装成反病毒软件的木马程序，运行后会弹出虚假报警恐吓用户，提示用户如果想彻底查杀家族必须购买软件，并提示用户使用信用卡支付，通过扰乱用户正常使用电脑的策略，骗取用户对软件付费。（威胁等级中）
		Trojan[Downloader]/Win32.Cabby	此威胁是一种具有下载行为的木马类程序，该恶意代码通过钓鱼网站、未知链接、下载黑客发布的免费软件及垃圾邮件附件等形式进行传播。（威胁等级中）

IC3 报告称，2015 年企业是网络犯罪的重灾区

Tom Spring/ 文　安天公益翻译小组 / 译

2015 年，企业遭受的电子邮件诈骗最为严重，美国公司的损失达到 2.63 亿美元。该数据来自 FBI(美国联邦调查局) 发布的《2015 年网络犯罪报告》，该报告指出了攻击美国企业和个人的各类网络犯罪。FBI 指出，去年，其互联网犯罪投诉中心 (IC3) 收到了 288,012 起投诉，总损失达到 10.7 亿美元。

总的来看，在 2015 年，企业电子邮件攻击 (BEC) 独占鳌头，超越了其他所有类型的犯罪。这类犯罪被归类为 BEC，它们利用社会工程学和计算机入侵技术，通过电子邮件发送金融诈骗信息，非法转移资金，导致大量的经济损失。

该报告指出：“犯罪分子通过伪造的电子邮件、拦截的传真或电话通信指示受害者重定向汇款。”FBI 报告称，在 2015 年，IC3 收到了 7,838 起 BEC 投诉，造成的经济损失超过 2.63 亿美元。

安全专家说，当涉及到网络防御时，这些类型的网络犯罪难以阻止。安全公司 Proofpoint 网络安全战略高级副总裁瑞恩·考莱姆伯指出：“BEC 攻击不涉及恶意软件。犯罪分子利用的是收件人的信任和涉及电子邮件的业务流程。”

根据 FBI 的报告，犯罪分子最常攻击有国外供应商或卫星办公室的企业。报告指出，通常情况下，这些 BEC 盗窃通过社会工程手段或某种类型的计算机入侵技术感染真正的商业电子邮件账户。

报告指出：“欺诈性汇款席卷很多国家的账户，其中一大部分是亚洲的。最常见的情况是，公司 CEO(首席执行官) 或 CFO(首席财务官) 的电子邮件账户被感染或伪造，要求向欺诈性账户电汇付款。”

在 Digital Shadows 公司首席执行官拉斯泰尔·帕特森看来，这些趋势是真实的。他说，他的公司发现了针对首席执行官、首席财务官、首席运营官、人事部门和会计人员精心炮制的复杂诡计。帕特森说：“攻击变得越来越复杂，犯罪分子们手段高明，他们监控 CEO 的社交媒体，在最佳时间采取行动，伪造汇款要求。”

根据 IC3 的报告：“2015 年，很多受害者报告称，伪装为律师或律师事务所的人士联系他们，指示他们执行机密或紧急的电汇。”

安全公司 Synack 的研究总监帕特里克·沃德尔表示，伪造来自 CEO 的电子邮件是一种高明的战术。“其利用了人性的另一个弱点：员工很少质疑来自 CEO 的电子邮件或要求。”沃德尔说。随着计算机部署反漏洞利用减灾措施，计算机更加难以攻破，网络的保护措施也更加完善。此时，人为因素就成了一个软肋。

BEC 损失最严重的州是加利福尼亚 (6,450 万美元)、纽约 (2,350 万美元) 和佛罗里达 (1,960 万美元)。但是，对比 BEC 犯罪的成本和其他罪行的总成本，损失最严重的州并不是遭受攻击最严重的州。例如，2015 年，南卡罗来纳州 BEC 犯罪占网络犯罪损失的 47 %。紧随其后的是内布拉斯加州 (45 %)、密歇根州 (43 %) 和纽约 (41 %)。

在该报告中，FBI 还指出了另一类犯罪，即勒索软件和电子邮件账户攻击，这些攻击侧重于个人或专业人士 (并非企业)。

根据 2015 年的 2 万起投诉，个人数据泄漏的损失几乎达到 4,300 万美元。与此相反，企业数据泄露有近 2,500 起投诉，累计损失为 3,900 万美元。身份盗窃损失共计 5,700 万美元，虚假投资诈骗损失达到 1.19 亿美元。

根据该报告，漏洞利用相关的损失包括 2,453 起勒索投诉涉及的 160 万美元。针对个人的网络钓鱼和邮件诈骗导致的损失共计 120 万美元，DoS 攻击导致的损失接近 300 万美元。

Proofpoint 公司的考莱姆伯指出，较 2015 年，2016 年最大的转变和网络犯罪趋势是勒索软件。2015 年，勒索软件占被感染邮件样本的 3%。而 2016 年前 5 个月，勒索软件的比例已经达到了 30%。

原文名称	Cybercrime Hit Businesses Hardest in 2015，says IC3 Report
作者简介	Tom Spring，Threatpost 副主编。
原文信息	2016 年 5 月 27 日《Threatpost》发布，原文地址 https://threatpost.com/cybercrime-hit-businesses-hardest-in-2015-says-ic3-report/118345/
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。

安天发布《DDoS 攻击浅析》报告

近日，安天追影小组对 DDoS 攻击做了大量的研究与分析，通过威胁情报平台发现了一些活跃的 DDoS 样本，经过追影产品的自动分析，获取了其攻击目标。

由于 DDoS 样本的攻击目标是被控制端以发指令的方式控制的，所以捕获到的攻击目标在不同的时间会有所不同。追影小组捕获到的 DDoS 样本，在当时的攻击目标为某塑料钢管厂与某购物网站等有真实业务的网站。

DDoS 即分布式拒绝服务攻击，其包含了两层含义，一层为分布式攻击；另一层为拒绝服务攻击。所谓拒绝服务攻击即凡导致合法用户不能访问服务的行为，均可被称为拒绝服务攻击，较典型例子为造成一个公开的网站无法访问。攻击者不断提出消耗服务器资源的请求，造成服务器繁忙，直到合法的用户请求无法被处理。但大型的网站服务器性能较强，对于普通的攻击可以应付，黑客则通过控制不同地区大量的“肉鸡”来同时攻击目标网站，这种方式即被称为“分部式”。

DDoS 攻击的用途目前可总结为以下几类：第一类是利用 DDoS 攻击进行勒索，主要目标为在线交易市场或博彩网站等，一般的攻击方式为先短期试探性攻击，然后发出勒索短信或邮件进行勒索，若不支付赎金，则在网站业务最繁忙的时段进攻击，从而影响网站的销售额迫使受害者缴纳赎金；第二类为打击同行业的竞争者，包括商业与政治上的竞争对手，追影小组捕获到的攻击事件应该属于这一类；第三类为带有报复性质的攻击。

不同于现实世界肉眼可见的攻击，藏匿于网络世界的攻击更加难以追查。对于 DDoS 攻击的治理，切断源头是最有效的方法，即定位控制端，治理控制端域名或 IP，安天追影产品目前已具备该功能，并且可检出未知的 DDoS 威胁。

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、关联分析鉴定器、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、美国软件交叉索引 (NSRL) 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 BD 静态分析鉴定器、关联分析鉴定器、静态分析鉴定器、动态行为鉴定器、智能学习鉴定器将文件判定为木马程序。

该文件具有以下行为：删除自身、获取 CPU 信息、释放 PE 文件、获取系统内存、打开自身进程文件、访问 dns、复制自身文件、创建服务、连接网络、创建特定窗体、获取驱动器类型、独占打开文件、获取计算机名称、获取主机用户名称、启动服务、请求加载驱动的权限、疑似桌面控制。

文件名	E3884523AEB0DF847D8CAC0F553B1B4D
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	48 KB
MD5	E3884523AEB0DF847D8CAC0F553B1B4D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Rootkit]/Win32.Lapka
判定依据	静态分析

◆ 危险行为

行为描述	危险等级
删除自身	★★★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=E3884523AEB0DF847D8CAC0F553B1B4D

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取 CPU 信息	★★	释放 PE 文件	★
获取系统内存	★★	打开自身进程文件	★
访问 dns	★	复制自身文件	★★
创建特定窗体	★	创建服务	★
获取计算机名称	★	连接网络	★
启动服务	★	获取驱动器类型	★
获取 CPU 信息	★★	独占打开文件	★
请求加载驱动的权限	★	获取主机用户名称	★
疑似桌面控制	★	请求加载驱动的权限	