安天周观察

主办：安天　2016 年 8 月 22 日（总第 53 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

黑龙江省委常委、组织部部长杨汭莅临安天总部参观指导

8 月 16 日，黑龙江省委常委、组织部部长杨汭一行莅临安天哈尔滨总部参观指导，并听取了我司发展近况及相关项目情况汇报。

在展示厅里，安天相关负责人向考察组介绍了安天近期发展情况，包括公司的发展目标、定位、团队能力储备以及在产品创新和知识产权等方面所取得的成果。介绍了国内网络威胁疫情趋势和遭受网络攻击威胁情况的分布。展示了安天反病毒等领域的核心技术积累和高级威胁检测以及态势感知产品线。汇报了安天历年参与重大安全响应事件的工作情况。

杨汭部长对安天所取得的技术成果给予了肯定，听取了安天对于网络安全防护工作提出的建议。最后，杨汭部长指出，由于信息技术发展而带来的网络安全问题日渐突出，希望安天能够继续钻研自主创新的核心网络安全技术，发挥自身的技术能力优势，为进一步的网络安全防护工作做出贡献。

“爱”的味道再一次温暖安全业界

“不为盲目追随完美和极致，只为专注安全、品味希望”，南俊苹果贴在一年后的今天再次被业内大量转发。今年，安天采购了 100 箱南俊苹果与每位同事分享，希望再一次能把这份关爱传递下去，一起为南俊加油，愿苹果的甘甜流入每位同事的心里，望每一位身处困难的人都能“苹”安、幸福。

南俊曾是中国电信安全服务中心的一名安全从业者！三年前一次意外交通事故，他被迫离开了工作岗位。经过艰苦康复，他于 2015 年带着家乡的苹果回到安全圈，在同事们看来，南俊苹果代表着又一次奋斗，是一份希望的味道，为他点赞！

◆首届网络空间战略论坛暨中国信息安全网上线发布会召开在即

8 月 27 日，首届网络空间战略论坛暨中国信息安全网上线发布会将在京召开。发布会由中央军委科技委、国家军民融合委员会、中国互联网发展基金会、中国信息安全测评中心联合指导，《中国信息安全》杂志社、北京华夏文化交流促进会、八九八九创新空间（北京）科技有限公司主办。安天技术负责人将发表题为《网络空间安全的能力层次和民力转化》演讲。

◆XCon2016 即将召开

8 月 29–30 日，第十五届安全焦点信息安全技术峰会 XCon2016 将在北京诺京酒店召开。来自全世界的信息安全专家、学者、研究员以及相关专业人士受邀参会，发表演讲。29 日，安天代表陈传文将发表题为《移动 App 通信协议安全详解》的演讲；30 日，安天代表桑胜田将发表题为《SRAM 型 FPGA 的信息安全风险浅析》的演讲。

◆DiskFiltration：利用硬盘声音窃取未联网设备上的数据

近日，以色列本·古里安大学的研究人员又发现了一种新方法窃取未联网设备上的数据。这种方法被称为 DiskFiltration，利用未联网目标电脑上的硬盘声音信号来窃取数据。它的工作原理是通过设法操纵机械硬盘的执行机构 (Actuators) 以非常特殊的方式运动，生成电脑上储存的密码、密钥和其他敏感数据的声音，并传输给附近的麦克风。这项技术的工作距离是 6 英尺，传输速率是每分钟 180 比特，足以在 25 分钟内窃取 4096 位的密钥。（来源：http://www.solidot.org/story?sid=49304）

◆美国约 20 家知名酒店 POS 机遭恶意软件感染

近日，美国约 20 家酒店的客户银行卡信息泄露，受影响的酒店包括万豪酒店、凯越酒店、洲际酒店、喜达屋、喜来登和威斯汀连锁酒店。酒店方称，在公司的系统中发现能够从任何销售终端上窃取信用卡交易数据的恶意软件，从 2015 年 3 月 1 日至 2016 年 6 月 21 日期间的大约 8000 笔交易受到该恶意软件的影响。酒店方就此次事件进行道歉，并称他们已经通过安装软件来加强数据安全，客户可以放心在任何酒店使用信用卡。但有最新报告指出，有些酒店是在该恶意软件被公布之后受影响的，似乎之前的教训并没有让其他酒店建立足够的安全措施。最终，酒店方回应已经通知联邦当局，并采用新的支付处理系统。（来源：https://securityledger.com/2016/08/20-top-us-hotels-hit-by-fresh-malware-attacks-zdnet/）

每周安全事件

类 型	内 容
中文标题	“食尸鬼行动”攻击 30 多个国家超过 130 家企业
英文标题	“Operation Ghoul” Targets Industrial，Engineering Companies In 30 Countries
作者及单位	Jai Vijayan；Darkreading
内容概述	近日，一个组织严密的网络犯罪团伙对超过 30 个国家逾 130 家企业开展工业间谍活动。绝大多数受害者为工业领域的中小型企业 (30-300 员工)。大多数目标企业活跃在工业领域，比如石油化工、海军、军事、航空航天、重型机械、太阳能、刚铁、泵、塑料等行业。该组织主要将目标局限在活跃于工业领域的企业，但不具体针对一个国家。攻击范围遍布全球：西班牙 (25 起)、巴基斯坦 (22 起)、阿联酋 (19 起)、印度 (17 起)、埃及 (16 起) 等。
链接地址	http://www.darkreading.com/attacks-breaches/operation-ghoul-targets-industrial-engineering-companies-in-30-countries/d/d-id/1326659

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 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	Trojan/Android.Mazig.a[rog，exp] 2016-08-15	该应用运行后会请求激活设备管理器，隐藏图标，私自联网访问指定网址，点击后会跳转访问推送广告页面或者是色情页面，会造成用户资费消耗，建议卸载。(威胁等级高)
		Trojan/Android.mrecorder.a[prv，rmt，spy]2016-08-17	该应用是一款间谍程序，安装后会隐藏图标，会获取用户短信、通话记录、地理位置信息、发送远程控制指令、录像拍照信息及 WhatsApp 消息记录，上传到远程服务器，造成隐私泄露。(威胁等级高)
		G-Ware/Android.Niaoqi.a[rog，exp] 2016-08-17	该应用程序安装后会诱导用户安装恶意子包，通过积分墙的形式推送大量广告，会造成资费损耗，建议立即卸载。(威胁等级低)
		Trojan/Android.Paccy.a[exp，rog] 2016-08-18	该应用程序伪装成系统程序，安装后无图标，会运行释放风险子包，静默安装广告插件，执行插屏广告推送，会影响用户正常体验，造成用户资费消耗，建议及时卸载。(威胁等级高)
		Trojan/Android.AndFraspy.c[prv，spy]2016-08-18	该应用为窃取用户隐私的间谍程序，会实现“假关机”，窃取用户的联系人、通话记录、浏览器记录、短信息、位置等信息，并且私自发送短信、删除短信。会造成用户隐私泄露，建议卸载。(威胁等级高)
	较为活跃的样本	Trojan/Android.SMSKey.b[exp]	该应用包含恶意插件，运行后会上传手机固件信息，获取扣费数据信息，执行发送付费短信并拦截回执短信，后续设置守护进程，存在一定安全风险，会造成用户经济损失，建议卸载该程序。(威胁等级中)
		Trojan/Android.Marcher.b[exp，prv，sys，rmt]	该程序会伪装成知名应用，运行后会诱导激活设备管理器并隐藏图标。诱骗用户输入银行卡账号密码等相关信息上传到远程服务器，同时联网获取配置信息进行拨打电话、发送短信、拦截短信等操作，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.SmsThief.ao[prv，fra]	该应用运行后会诱导用户输入姓名和邮箱，上传姓名和邮箱信息。监听短信，转发用户接收的短信，会造成用户隐私泄露和资费损耗，建议卸载。(威胁等级中)
		G-Ware/Android.HiddenAds.ad[rog，exp]	该应用运行后会弹窗诱导用户点击安装推广浏览器，之后隐藏图标，加载广告，会造成用户资费损耗，建议卸载。(威胁等级低)
		G-Ware/Android.Supe.b[rog，exp]	该应用伪装成系统应用，安装后无图标，程序运行后会私自联网下载大量的色情类图标和色情应用，创建大量的桌面快捷方式，会造成用户资费消耗，建议卸载。(威胁等级低)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Word 远程代码执行漏洞 (CVE-2015-0097)(MS15-022)	Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。Office 解析构造的 Office 文件时存在 Local Zone 相关错误，通过构造 Office 文件，攻击者利用此漏洞可以执行任意代码，破坏内存。(威胁等级高)
	较为活跃的样本	Trojan[Downloader]/MSWord.Steamilik	此威胁是一类可以下载恶意代码的木马家族。该家族样本为 Word 宏病毒，运行后会连接网络下载恶意代码并运行。(威胁等级中)
		Trojan[Spy]/Win32.Selltim	此威胁是一类间谍软件，属于木马家族。该家族样本会将载荷隐藏在资源中，运行后会连接远程服务器接受恶意操作，可以下载其他恶意代码、会上传用户敏感信息等。(威胁等级中)
		Trojan/Win32.Emospam	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后会复制自身到 %TEMP% 下并自我删除，会收集系统信息并上传至远程服务器。(威胁等级中)
		GrayWare[AdWare]/Win32.Linkury	此威胁是一种广告类木马程序，属于灰色软件家族。该家族样本运行后会安装浏览器搜索工具栏并修改浏览器主页，会弹出广告，占用系统资源，影响用户使用。(威胁等级低)

攻击遥控钥匙，解锁数百万汽车

Tom Spring / 文　安天公益翻译小组 / 译

近日，学术研究人员又指出了一种新的汽车攻击。这种攻击涉及数百万的大众、福特和雪佛兰汽车。这些汽车依赖过时的遥控钥匙技术，即使是“水平一般的黑客”也能侵入汽车系统并进行解锁。鉴于此，车主在后备箱中放置贵重物品之前可要三思了。

一份介绍该攻击的报告指出：“该攻击影响了全球数百万的汽车，我们的研究能够解释一些涉嫌盗窃已锁车辆的未解保险案件。”研究人员弗拉维奥·D·加西亚 (Flavio D. Garcia)，大卫·奥斯瓦尔德 (David Oswald)，蒂莫·卡斯帕 (Timo Kasper) 和皮埃尔·帕里德斯 (Pierre Pavlid è s) 计划在本周德克萨斯州奥斯汀举行的 USENIX 安全讨论会上介绍该研究。

《路透社》指出，大众汽车并没有对此进行争辩，表示：其目前车辆不会受到该问题的困扰。

研究人员表示黑客可以使用廉价的技术设备侵入遥控钥匙进入系统。“在分析过程中，我们使用了各种设备，包括软件定义无线电 (HackRF，USRP，rtl-sdr DVB-T USB) 和廉价的射频模块。这些简单的设置由电池供电，花费 40 美元，

能够窃听并记录滚动码，模拟钥匙，并进行反应干扰。”

研究人员还指出，该攻击利用了两个漏洞，一个漏洞允许攻击者解锁 1995 年以来几乎每一种型号的大众汽车；另一个漏洞影响到阿尔法·罗密欧、雪铁龙、菲亚特、福特、三菱、日产、欧宝和标致汽车的遥控钥匙。

这两种攻击都在距离目标汽车 300 英尺范围内，使用修改的 Arduino 无线电装置，来拦截汽车遥控钥匙的代码。第一种漏洞使用窃听装置，来恢复所有大众汽车使用的固定加密密钥组。研究人员说，利用 Arduino，他们只需在车主用遥控钥匙打开汽车时窃听一次，就能破解代码。

第二种漏洞与遥控钥匙加密方案 HiTag2 有关。因为算法中存在漏洞，研究人员能够轻松地破解 HiTag2 加密系统。研究人员使用 Arduino 无线电设备，拦截了遥控钥匙以滚动模式出现的 8 个密码。研究人员写到：“平均而言，通过大约 1 分钟的计算，几个窃听得来的滚动码 (4 到 8 个)，我们就能恢复密钥。”

汽车攻击专家指出，大众汽车遥控钥匙的安全性不严格甚至不存在。推而广之，整个汽车产业都是如此。IOActive 的高级安全顾问科里·图恩最近发布了一份关于汽车安全的报告，他指出：“大众汽车绝非特例。在我们研究的每一个汽车系统中，我们都发现了这种类似的安全问题。他们要么重用密码，依靠硬编码的凭证；要么未禁用开发者后门程序。”

研究人员说，用于侵入汽车的必要设备成本很低，而且在地下市场作为黑盒工具包出售。他们总结说：“因此，这些攻击是高度可扩展的，即使水平低下的黑客也可以执行。”

图恩指出，坏消息是修复该问题将会非常困难。“解决方法非常复杂，需要更新数千万受影响的组件。大众汽车最大的错误是，没有正确理解和正确实施加密。”他补充说，诸如大众的汽车制造商永远不应认为其设备中的数据是安全的。

原文名称	Key Fob Hack Allows Attackers To Unlock Millions Of Cars
作者简介	Tom Spring，《Threatpsot》副主编。
原文信息	2016 年 8 月 12 日发布于《Threatpost》 原文地址 https://threatpost.com/key-fob-hack-allows-attackers-to-unlock-millions-of-cars/119846/
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《“Backdoor.Remsec”样本分析报告》

近日，安天追影小组在梳理网络安全事件时，发现“Backdoor.Remsec”木马并对其做了简要分析。自 2011 年 10 月以来，Strider 网络间谍组织使用名为“Remsec”的后门木马，进行了广范围的企业攻击。从操作层面看，该组织与 Flamer（火焰）病毒组织有共同点。因为这两个组织均使用了基于 Lua 模块的恶意软件。“Backdoor.Remsec”通过感染主机从而窃取受害者的敏感信息，利用获取的信息会对受害者造成物理和财产破坏，如获取受害企业的相关商业机密、进行财产盗窃等。

经安天追影小组分析，“Backdoor.Remsec”后门木马使用 Microsoft Visual C++ 6.0 编写，样本可以感染 windows 系列操作系统，系统兼容性强，可以完全控制被感染主机，实现对任意文件的读写删除、发送远程命令等。该木马具有高隐藏性、高潜伏性、高危害性。

“Backdoor.Remsec”木马通常隐藏在 MSAOSSPC.dll 文件中，利用调用 MSAOSSPC.dll 文件的正常软件实施感染。而且作者针对该木马进行了二次加解密的加壳保护。该后门木马自身包含：keylogging、network listener、HTTP backdoor 和 network loader 等功能模块，对于所有模块，载入程序只会在需要时载入。此外，该木马能监听本地网络套接字，并以多种方式将后门向控制与命令服务器打开。该木马采用 Lua 模块化设计并且其大部分功能通过网络传输，只驻留在内存中，不允许本地文件驻留，因此大部分杀软难以检测。另外，该木马的攻击目标较少，使得隐秘攻击能够长达 5 年之久，而未被察觉。

目前，该类恶意代码已经可以被安天追影产品检出。从大量的分析事件总结发现恶意代码的感染手段千变万化，恶意目的各不相同，为了避免企业与个人的损失。安天提醒网络使用者：不要随意点击不明来源的邮件或社交网站中的链接，不要轻易下载邮件中不明来源的附件，养成及时更新操作系统和软件应用的好习惯。

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。

文件名	234E22D3B7BBA6C0891DE0A19B79D7EA
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	132 KB
MD5	234E22D3B7BBA6C0891DE0A19B79D7EA
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[:HEUR]/Multi.Remsec
判定依据	静态分析

危险行为

行为描述	危险等级
扫描 445 端口尝试访问系统共享文件夹	★★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=234E22D3B7BBA6C0891DE0A19B79D7EA

最终依据 BD 静态分析鉴定器、静态分析鉴定器将文件判定为木马程序。

该文件具有以下行为：扫描 445 端口尝试访问系统共享文件夹、查找指定内核模块、连接网络、填充导入表（疑似壳）、独占打开文件。

其他行为

行为描述	危险等级	行为描述	危险等级
查找指定内核模块	★	连接网络	★
填充导入表（疑似壳）	★★	独占打开文件	★

网络监控

访问 IP			
IP 地址	端口	归属地	域名
192.168.0.1	445	N/A	N/A

TCP 信息			
源 IP	源端口	目的 IP	目的端口
127.0.0.1	445null	192.168.0.1	445

TCP 信息			
源 IP	源端口	目的 IP	目的端口
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.97	68