安天周观察

主办：安天　2017 年 7 月 24 日（总第 96 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天荣获通信网络安全服务能力评定双证书

日前，安天获中国通信企业协会颁发的“通信网络安全服务能力评定证书（应急响应一级）、通信网络安全服务能力评定证书（风险评估一级）”双证书，安天网络安全服务能力再获认可。

安天作为中国应急响应体系中重要的企业节点，在近年来的方程式、白象、WannaCry（魔窟）等重大安全事件中提供了先发预警、深度分析或系统的解决方案；并多次在重大网络事故和网络安全事件的响应中发挥关键作用，参加 9.3 抗战胜利日阅兵、G20 峰会等重大活动的安保工作，始终以做好国家、用户等各方面网络安全保障工作为己任。此次“通信网络安全服务能力评定（应急响应一级、风险评估一级）”资质认定，是对安天安全服务能力的肯定和激励。迄今为止，安天已拥有通信网络安全服务类的安全设计与集成一级资质、风险评估一级资质和应急响应一级资质。

展望未来，安天将进一步加强网络安全防护工作，提升网络安全技术产品能力和服务能力，为用户提供更高标准的安全服务。

安天助力黄河银行、哈尔滨银行构建终端安全有效防护体系

近期，安天连续中标宁夏黄河农村商业银行企业版杀毒软件采购项目和哈尔滨银行终端防护项目，助力客户构建终端安全有效防护体系，为国家关键信息基础设施安全防护提供强有力支撑。

银行的 ATM 机、现金存取机等金融终端面对日益凸显的勒索软件等新型攻击手段，存在极大的安全风险，终端的反病毒能力与应对新兴安全威胁的能力是提升终端安全的关键因素，加强金融终端有效防护能力势在必行。

安天结合黄河银行、哈尔滨银行的终端安全现状，以快速有效提升金融终端应对各种安全风险的防护能力为目标，部署安天智甲终端防御系统。安天智甲实现跨平台的一体化集中管理，帮助两大银行降低实施、管理和运维成本；具有强大的病毒查杀与多重防护功能，增强终端防护能力，构建有效防护体系；能够实时感知全网终端态势，提升安全事件响应速度，及时有效清除安全威胁。

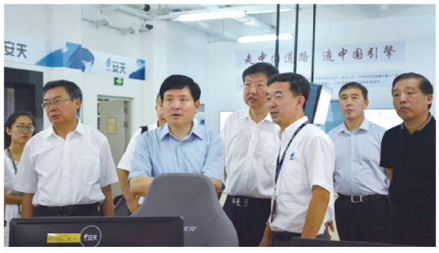
安天智甲终端防御系统采用私有云查杀架构、黑白双控检测机制、四级管控防护策略、提供主动防御、勒索病毒防护、漏洞监测与修复、安全基线、未知威胁防护、威胁追溯与清除、可视化管理、统计报表等功能，帮助用户精准识别、快速处理安全威胁，避免错杀漏杀，构建终端安全有效防护体系。

安天智甲完美适配各类型的用户终端，包括办公终端、服务器终端、虚拟化终端、专用设备终端（如：金融终端或工控设备等）和移动终端等，并提供全场景终端安全解决方案。全方位感知全网终端资产信息、终端安全态势；当发生安全事件时，可通过全网追溯、定点查杀等手段进行快速响应。

国家财政部副部长刘伟等一行莅临安天参观指导

持续发力“双创” 培育发展新动能，国务院第四次大督查工作正在进行。7 月 18 日上午，国家财政部副部长刘伟、国家财政部监督检查局副巡视员林启云、发展研究中心创新发展研究部副部长马名杰、国家教育部财务司副处长彭莉、国家财政部办公厅副处长杨光，在哈尔滨市市长宋希斌等领导陪同下莅临安天。

安天相关负责人向来宾介绍了安天的发展历程和现状，以及安天的技术分布，并展示了安天取得的专利资质和国家级应急响应资质。在安天应急响应中心，安天技术负责人介绍了安天持续与网络安全威胁对抗的情况，特别汇报了对高级威胁发现、捕获、分析方面所做的工作，重点介绍了安天针对 APT-TOCS、白象、方程式等攻击组织对我方 APT 攻击情况、所使用的攻击装备等的分析进展。



国家财政部副部长刘伟在听完安天情况的介绍后，对安天的艰难创业历程以及技术提升表示肯定，同时关切询问了安天的实习人员实习后的就业现状，他强调安天对国家做出很大贡献，更希望今后转化为效益，希望安天的人才培养、技术专利创新等方面有进一步提高，不断促进自身发展。

每周安全事件

类 型	内 容
中文标题	FreeRADIUS 曝出多个代码执行和 DoS 漏洞
英文标题	Code Execution，DoS Vulnerabilities Found in FreeRADIUS
作者及单位	Eduard Kovacs；Security Week
内容概述	近日，据外媒报道，研究人员针对 FreeRADIUS 进行了 fuzzing 测试，并发现其存在的 11 个安全问题，FreeRADIUS 的开发者又发现了额外的 4 个问题。这 15 个问题影响到版本 2 或 3，其中 5 个无法被利用，6 个影响到 DHCP 包解析器。这些漏洞均已在近期发布的 2.2.10 和 3.0.15 中修复。 此外，漏洞包括内存泄露、内存耗尽、缓冲区溢出、DoS 等。其中有个远程代码执行漏洞 CVE-2017-10984，影响到版本 3.0.0-3.0.14，以及漏洞 CVE-2017-10979 影响到 2.0.0-2.2.9。漏洞可通过发送恶意包来触发。如果 RADIUS 服务器位于公网，则问题会比较严重。
链接地址	http://www.securityweek.com/code-execution-dos-vulnerabilities-found-freeradius

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 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	相关描述
移动恶意代码	较为活跃样本	Trojan/Android.Agcr.a[rog，exp]	该应用安装无图标显示，程序运行会私自联网上传设备固件信息，释放子包文件并下载文件提权，造成用户资费消耗。（威胁等级高）
		Trojan/Android.timobox.b[exp]	该应用程序安装后会监听设备联网状态的变化情况，在网络可用时会检查当前版本并下载更新自身安装包，以及下载诸多不同类型的文件。另外其资源目录下的更新包包含广告推送行为。会造成用户流量资费损失，存在潜在的恶意应用或文件下载风险，建议谨慎使用。（威胁等级中）
		Trojan/Android.Vitamio.a[exp]	该应用程序伪装成正常应用，联网下载推广视频，诱导用户点击跳转推广页面，造成用户资费损耗，建议立即卸载。（威胁等级中）
		Trojan/Android.FakeInst.ej[prv，exp]	该应用程序伪装成色情、杀软等应用，运行后关闭 Wi-Fi，打开移动数据流量，诱导用户点击下载其他应用，获取用户手机号码和固件信息，加载风险网页，并触发 JS 文件模拟点击，后台拦截屏蔽短信，给用户造成隐私泄露和资费损失，建议立即卸载。（威胁等级低）
		Trojan/Android.LockScreen.y [rog，lck]	该应用程序伪装成其他应用，无实际功能，程序运行会强制置顶界面勒索用户付费解锁，建议卸载。（威胁等级中）
		Trojan/Android.Triada.p[exp，rog]	该应用包含色情敏感内容，运行后释放恶意子包并提权安装，上传手机固件信息和手机号码，后台加载广告，造成用户资费损耗和隐私泄露，建议不要安装。（威胁等级高）
		Trojan/Android.SmsSend.kq[exp]	该程序运行后隐藏图标，后台联网下载未知文件，造成用户资费损耗。（威胁等级高）
		Trojan/Android.Downloader.cl [rog，exp]	该应用伪装成正常应用，运行后隐藏图标，后台私自下载恶意应用和提权工具，提权并静默安装，造成用户资费损耗，建议不要安装。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Foxit Reader/PhantomPDF 信息泄露漏洞 (CVE-2017-8454)	Foxit Reader 是一款小型的 PDF 文档查看器和打印程序。Foxit Reader < 8.2.1、PhantomPDF < 8.2.1 版本存在越界读漏洞，远程攻击者通过构造 PDF 文档字体，获取敏感信息或执行任意代码。
	较为活跃的样本	Trojan[Downloader]/Shell.Agent	此威胁是一类具有执行 Shell 语句行为的恶意代码家族的统称。该家族的样本在执行后会利用 ShellExecute 等函数来执行特定的语句，对系统造成潜在危害。（威胁等级中）
		Trojan[Ransom]/Win32.Crysis	此威胁是一类可以加密用户文件并勒索金钱的敲诈者，特点是加密不影响系统运行的所有文件，目前俄罗斯、乌克兰、日本受到攻击。（威胁等级中）
		Trojan[DDoS]/Linux.Znaich	此威胁是一类可以发动分布式拒绝服务攻击的木马家族。该家族样本基于 Linux 系统，运行后向指定目标发起 DDoS 攻击。（威胁等级中）
		Trojan[Downloader]/Win32.Bedobot	此威胁是一种木马类程序。该家族样本运行后连接远程服务器下载恶意代码，目前其 URL 已经失效。它还可以遍历系统目录，分析下列后缀后的文件：.dbx、.wab、.mbx、.mai、.eml、.tbb、.mbox，收集系统中的邮件地址，回传至远程服务器。如果用户系统中包含重要的邮箱地址，危害会非常之大。（威胁等级中）

安全专家如何帮助患者保护医疗数据

Reza Chapman / 文　安天公益翻译小组 / 译

医疗行业在处理黑客攻击风险方面步履缓慢，数据泄露事件不断增加。安全专家必须更积极主动地保护患者的安全。

想象一下，一家当地医院的 IT 系统被黑客入侵，黑客威胁要在网上发布患者的姓名、地址和病历。在 2016 年 9 月，俄克拉何马州的6000名患者就遭遇了这样的事情。

埃森哲 (Accenture) 的最新研究发现，多达 26％的美国消费者遭遇了医疗数据泄露事件，在这其中，有 50％的人之后遭遇了医疗身份盗用。

目前，大多数消费者已经意识到在线交易的风险，但是很少有人意识到医疗身份盗用及其造成的损害。这就要求安全专家提供更强大的安全防护，要求医院在遭遇数据泄露期间和之前更好地进行数据管理。

身份危机

医疗数据包括测试结果和诊断，还包括社保号、出生日期、联系信息和驾照号码。这些信息共同构成了一个在线身份。黑客利用这些个人信息或医疗数据进行售卖，也可能以此威胁医院支付赎金，否则就“在网上公布数据”，或阻止医院访问这些重要信息。

其他行业正在加紧步伐应对数据安全，所以旨在窃取个人数据的黑客不得不换个目标。而且，大多数医疗信息是以电子方式存储的，可以追溯到几年前，因此对黑客来说医疗行业就是瓮中之鳖。

在 2016 年，医疗行业发生了 377 起数据泄露事件，占所有数据攻击事件的 34.5％。在 2017 年，截至 2 月中旬，已经发生了 144 次数据泄露事件。

一个合乎逻辑的问题是：“这些数据泄露事件发生在哪里，应该如何阻止？”根据埃森哲的研究，数据泄露事件最有可能发生在医院，其次是急诊室、药店、医生办公室和健康保险公司。通常情况下，医疗机构无法及时发现问题：在遭遇数据泄露的美国消费者中，有一半是因为信用卡对账单或利益解释有误而自己发现了数据泄露。只有三分之一是被医疗机构告知了数据泄露事件，只有 15％是被政府机构告知的。

安全专家了解医疗信息泄露的潜在机会，能够帮助医院系统和整个医疗行业加强防御措施，以确保消费者数据安全。

安全专家能做什么

医疗机构有义务保护医疗和金融数据。当安全措施不足时，就会导致数据泄露和数据窃取。埃森哲的研究表明，许多受影响的消费者会采取行动。受影响的受访者或者更换了医疗服务提供商 (25％) 或保险计划 (21％)，或寻求法律顾问 (19％)。根据最近的趋势和事件来看，安全专家的作用会越来越重要。

许多消费者了解数据泄露对其财务状况和健康状况的影响。每起医疗身份盗用事件的受害者平均损失为 2500 美元，与信用卡数据泄露不同，身份盗用的受害者通常没有追回损失的权利。埃森哲的调查发现，当医疗机构主动与消费者进行沟通时，追回损失的几率仍然很高。这说明提前准备好应对潜在攻击的重要性，医疗机构能够迅速采取行动，在事件发生期间或之后帮助减轻消费者的恐惧心理。

医疗服务提供商要更加认真地看待数据窃取了，安全专家也需要在患者和医疗机构之间建立更强大的信任关系。以下几个措施能够帮助保护消费者数据：

◆ **敦促消费者监督医疗记录并阅读所有声明**。如果病历不准确，那么他们的数据可能与其他人的混合了。敦促患者密切关注医疗服务提供商给出的病历和声明，并要求他们至少每年一次提供摘要。

◆ **提醒消费者查看其信用报告**。信用报告的任何差异都有可能意味着消费者的医疗数据已经受到了侵害。

◆ **不要过分分享信息**。消费者只应该提供所需的最低限度的个人信息，例如医疗服务提供商不需要患者的社保号。消费者还应该警惕虚假通信：在 2015 年的 Anthem 数据泄露事件之后，受害者称接到了钓鱼电话和电子邮件。

◆ **立即发出警报**。如果消费者发现任何异常，应立即通过用户友好的渠道告知医疗服务提供商或保险公司。

原文名称	How Security Pros Can Help Protect Patients from Medical Data Theft
作者简介	Reza Chapman，埃森哲全球医疗业务网络安全总监，负责为提供商、健康保险公司和业务伙伴开发和推动安全产品。
原文信息	2017 年 7 月 13 日发布于 Dark Reading 原文地址 http://www.darkreading.com/attacks-breaches/how-security-pros-can-help-protect-patients-from-medical-data-theft/a/d-id/1329326?
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《Sorebrect 勒索软件样本分析报告》

近日，安天 CERT（安全研究与应急处理中心）分析人员发现，近期出现了一个新的勒索软件家族 Sorebrect。与大部分其他勒索软件不同的是，该家族勒索软件没有文件实体，且采用代码注入的方式进行感染和文件加密。多种技术的结合，使它比其他勒索软件更具备威胁性。

Sorebrect 使用无文件实体和进程注入技术，同时使用 wevtutil 删除被感染系统的日志以达到阻碍分析和取证的目的。Sorebrect 勒索软件较突出的特点是对 PsExec 的滥用。PsExec 是一个合法的 Windows 命令行实用程序，可让系统管理员在远程系统上执行命令或运行可执行文件。虽然 PsExec 和 RDP 都能够通过远程协议执行命令或安装文件，但是相较于 RDP，利用 PsExec 更为简单。滥用 PsExec 的恶意代码，除了 Sorebrect 外，还有 Petya、SAMASAM 及 Petya 的衍生物 PetrWrap 等。Sorebrect 勒索软件对 PsExec 无文件实体和代码注入等技术的结合使用，可使攻击者能够执行远程命令，而非使用交互登录会话或将恶意软件手动传输至远程机器设备。此外，被感染机器使用 PsExec，攻击者可以获取机器管理员的口令。

除加密本地文件外，Sorebrect 还可扫描网络上其他计算机的共享文件夹，如果文件夹设置为任何用户都有读写权限，那么该文件夹也将被加密。

针对 Sorebrect 勒索软件的特性和主要针对目标，安天为用户提出以下几点防御措施：

- 限制重要资料共享和读写权限；
- 加强设备管理员口令强度；
- 限制 PsExec 权限；做好重要文件备份；
- 培养从业人员网络安全意识，提升企业内部安全操作标准。

目前，研究人员在部分中东国家、加拿大、中国、美国等国家和地区发现了 Sorebrect 勒索软件的感染迹象，受影响的行业主要包括制造业、科技和电信企业等。目前，Sorebrect 样本已由安天追影威胁鉴定器检出。

木马程序

安天【追影威胁分析系统】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：

文件被页面手工提交发现，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 (Windows7) 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 BD 静态分析鉴定器、静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

根据动态行为 (Windows7) 得出该文件具有以下行为：其他进程写入可疑数据、遍历进程、结束进程。

根据动态行为（默认环境）得出该文件具有以下行为：其他进程写入可疑数据、延时、获取系统版本、获取驱动器类型、查找指定内核模块、创建挂起的进程、查询 windows product key、获取计算机名称、填充导入表（疑似壳）、获取主机用户名称、创建特定窗体、请求加载驱动的权限、获取 socket 本地名称、查找浏览器进程、连接网络、独占打开文件、获取系统内存。

文件名	4142ff4667f5b9986888bdcb2a727db6a767f78fe1d5d4ae3346365a1d70eb76
文件类型	BinExecute/Microsoft.PE[:X86]
大小	999 KB
MD5	83E824C998F321A9179EFC5C2CD0A118
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.BTSGeneric
判定依据	静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=83E824C998F321A9179EFC5C2CD0A118

运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office 2007、flash、wps、FoxitReader、adobe reader

危险行为

行为描述	危险等级
其他进程写入可疑数据	★★★

其他行为

行为描述	危险等级	行为描述	危险等级
遍历进程	★	结束进程	★★