安天周观察

主办：安天　2016 年 10 月 17 日（总第 60 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天在全国保密技术交流大会展示全线产品体系

10 月 13 日 -15 日，由中国保密协会主办的 2016 年保密技术交流大会暨产品博览会在青岛举行，“保密技术交流大会”是专业性最强、规模最大、供需双方最全的信息安全保密科技的行业盛会。

本次大会以“促进技术创新，加快成果转化”为主题。安天全线产品体系，包括探海威胁检测系统、追影威胁分析系统、智甲终端防御系统、镇关威胁阻断系统以及态势感知平台等悉数亮相。探海威胁检测系统 (PTD) 可以针对网络出口和关键网段进行高速的流量解析、还原与精确检测；智甲终端防护系统 (IEP) 可以基于传统企业杀毒和“白名单 + 安全基线”两种模式进行部署，有效改善桌面和服务器的安全防御能力；对于探海、智甲捕获的可疑文件，可以投放到追影威胁鉴定系统中进行深度动静态分析，而追影分析后所形成的远控等信标规则可以同步镇关威胁阻断系统进行拦截。相关产品可以通过安天态势感知与监控预警产品进行集中管理，并获得安天的后台能力和威胁情报的有效支撑。

在展会期间，召开了第二十六届全国信息保密学术会议，安天负责人肖新光发表了技术报告“高级持续性威胁 (APT) 背景下的保密工作的思考”。报告从分析中国地缘安全形势，解读了 APT、CNE、CNA 等不同属于的概念内涵。并从安天捕获分析来自不同对手的多个 APT 攻击案例入手，分析了 APT 攻击中的“武器库”、“战场环境”、“商业军火”，供应链安全等问题。报告引用安天在“白象”攻击组织分析报告，强调“大国的网络安全能力要由攻击者和窥视者检验”“但来自对手的‘检验报告’必然姗姗来迟”。在反 APT 攻击问题上，必须以体系化防御对决体系化进攻，而没有银弹和永动机。

工信部网安局副巡视员隋静一行莅临安天参观指导

10 月 10 日，工信部网安局副巡视员隋静一行莅临哈尔滨安天总部进行了实地参观，并听取了安天发展近况汇报。

安天相关负责人介绍了安天的发展状况和历史以及在技术创新和知识产权方面取得的成果。并展示了安天安全威胁感知捕获系统和可视化平台。介绍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威胁态势感知展品线，汇报了安天历年参与重大安全响应事件的工作情况。

安天 CERT 负责人李柏松向隋静重点介绍了 CERT 部门的定位和运营情况，隋静表示对安天发出的“每日安全简讯”比较关注，她希望安天能更多的提供产业相关的新信息，与相关部门及时沟通。

隋静表示未来网络安全会很重要，要解决好网络安全威胁问题，并对安天坚持走到今天表示肯定，希望安天为网络安全防护提出更好地解决方案，为国家网络安全做出贡献。

新型勒索软件“DXXD”使用 Windows 登录界面显示赎金信息

近日，一款名为 DXXD 的新型勒索软件使用 Windows 的法律公告屏显示赎金信息。Windows 法律公告屏是 Windows 登录界面出现之前的提示信息，在用户使用电脑前显示各类法律声明及其他消息。

虽然用户本可以通过按“确定”键跳过这些提示，但屏幕仍会显示赎金信息引起用户的注意。遇到这种情况的用户电脑中的文件会被 DXXD 勒索软件加密，该勒索软件于九月底出现。

除了明显的赎金信息，勒索软件还在被感染的电脑上添加了两个注册表项。识别 DXXD 非常简单，因为所有被它加密的文件名后都有“dxxd”的字符串，例如“photo.png”会变为“photo.pngdxxd.”。

（文章来源：http://www.cnnvd.org.cn/news/show/id/7743）

每周安全事件

类 型	内 容
中文标题	国际原子能机构确认德国核电站遭破坏性网络攻击
英文标题	Shocking, a German nuclear plant suffered a disruptive cyber attack
作者及单位	Pierluigi Paganini；Securityaffairs
内容概述	近日，国际原子能机构 (IAEA) 相关人员表示，德国一家核电站两三年前曾遭遇“破坏性”网络攻击。此类设施的安全威胁正在逐渐增高，除了愈演愈烈的网络攻击，还有人试图从核电站偷盗铀原料制造脏弹 (放射性炸弹)。有关人员表示：“这可不是我们臆想出的威胁，大家对此事必须重视起来。IAEA 发现的这些偶发事件可能只是冰山一角。” 近些年来，网络攻击对社会的威胁越来越大，黑客已经掌握了控制工业设施的方法，一旦他们攻破核电站的防线，后果不堪设想。而调查显示，今年 3 月布鲁塞尔恐怖袭击的最初目标就是比利时的核设施。今年 4 月，德国核电站网络系统得到了全面升级，而此前它们就遭到过电脑病毒的感染。
链接地址	http://securityaffairs.co/wordpress/52116/security/nuclear-plant-attack.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 9 个移动平台恶意代码和 4 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.igpi.a[rog，sys，exp]2016-10-10	该应用伪装成系统应用，安装后无图标，运行后会获取 root 权限加载释放子包到系统文件目录，私自联网上传设备固件信息并下载恶意文件，造成用户资费消耗。(威胁等级高)
		Trojan/Android.ystg.a[rog，pay]2016-10-13	该应用会伪装成系统应用，安装后无图标，程序运行后会私自发送订购短信，监听短信并拦截指定短信，造成用户资费消耗。(威胁等级中)
		Trojan/Android.Tigde.a[prv] 2016-10-14	该应用程序运行后会隐藏图标，获取用户通话记录、录音、经纬度信息并上传至远程服务器，会造成用户隐私泄露。(威胁等级中)
		RiskWare/Android.xmxx.a[exp]2016-10-14	该游戏应用程序经过重打包，会植入支付插件，建议谨慎使用以免造成资费损失。(威胁等级低)
	较为活跃的样本	Trojan/Android.SmsSend.kk[prv]	该应用运行后会隐藏图标，监听短信信息，会获取用户收件箱信息，私自联网和发送短信，造成用户隐私泄露。建议卸载。(威胁等级中)
		G-Ware/Android.HiddenAds.ae[rog，exp]	该应用程序运行后会隐藏图标，后台会联网获取广告配置信息，推送广告，会造成用户资费损耗，建议谨慎使用。(威胁等级低)
		Trojan/Android.Triada.l[exp，sys]	该应用程序会伪装成正常应用，安装后无图标，运行后会获取 root 权限，并静默卸载应用；同时包含私自下载安装程序的风险方法，会造成用户资费损耗和影响系统安全，建议立即卸载。(威胁等级高)
		Trojan/Android.AnalyzerSpy.b[prv，rmt，spy]	该应用运行后会请求激活设备管理器禁止卸载，窃取短信、通话记录信息，后台会拍照录音，开启后门，造成用户隐私泄露，建议及时卸载。(威胁等级高)
		Trojan/Android.SmsSend.km[prv，exp]	该应用会私自发送恶意扣费的短信，且拦截回复的指定内容的短信，并联网上传设备信息，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 Memory Corruption Vulnerability-CVE-2016-7193(MS16-121)	Microsoft Office Memory Corruption Vulnerability - CVE-2016-7193 (MS16-121) 当 Office 无法处理 RTF 时，会导致 RTF 远程漏洞执行。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。(威胁等级高)
	较为活跃的样本	Trojan[Downloader]/Win32.Cafys	此威胁是一种具有下载行为的恶意木马类程序。它感染计算机后，如果用户试图打开相关文件或者应用程序，就会弹出错误警告。它不仅可以阻止你使用一些服务并会影响电脑的其他功能。(威胁等级中)
		Trojan[Downloader]/Win32.Dyfuca	此威胁是一种具有下载行为的恶意木马类程序。该家族会收集感染主机访问过的站点详细信息，并发送给远端的服务器。该家族会连接服务器，下载恶意程序并运行。(威胁等级中)
		Trojan[Ransom]/Win32.BrowHost	此威胁是一种勒索赎金的木马家族。它可以加密用户数据并要求用户付费解密，否则数据就会被破坏，有一定威胁。(威胁等级高)

大数据安全问题威胁用户隐私

Jungwoo Ryoo / 文　安天公益翻译小组 / 译

随着大量个人信息被越来越强大的计算机收集，巨大的数据集——即大数据——可能被合法使用也有可能被滥用。

潜在问题的大小

首先，由于大数据安全事件牵涉大量的人，因此风险比以往都要高。例如，2014 年阿肯色大学的专业开发系统遭到入侵，5 万人受到了影响。

即使从安全专家的角度看来，保护大数据集也是艰巨的。部分原因在于当前用于信息存储、处理的底层技术不够先进。

像亚马逊这样的大数据公司极度依赖分布式计算，通常靠分散在世界各地的数据中心完成。亚马逊全球计算运营中心有 12 个分区，每个分区包含多个数据中心，但是这样一来，数万台在其中的服务器很可能会遭受物理攻击和持续的网络攻击。

访问控制遇到的困难

单点访问是控制访问信息或物理空间的最好方法之一，与控制数百个访问点相比单点访问更加容易确保数据安全。然而实际情况是大数据的存储分布地域极广，这与该原则相悖。而且，由于数据量大、分布广以及访问路径多，使得它遭受攻击的风险更高。

另外，很多复杂的软件组件对数据安全问题不够重视，包括部分公司的大数据设施存在隐患，这就为潜在的攻击打开了通径。

用户需求推动安全和隐私的保护

对用户来说，要求收集和使用大数据的机构通过诸如条款，服务水平协议以及安全信任协议等媒介来提高安全防护级别，这很重要。

保护个人信息公司可以做些什么？它可以采取，例如加密、访问控制、入侵检测、备份、审查和公司程序等对策避免个人信息失窃或落入不法分子之手。不过，提升安全级别也可能侵犯你的隐私：它给个人信息大量收集提供了正当的借口，例如员工在工作电脑上的网页浏览记录。

当执法机构以提高安全防护的名义收集信息时，其实每一个人都被当做潜在的罪犯或恐怖份子，执法机构害怕个人信息最终会被用来攻击自己。“任何人都不可信”的基本安全原则可以用来解释执法机构的地毯式监视。被收集的个人信息，会放到易被滥用与盗窃的信息库中，如国家安全局员工涉嫌窃听事件。但是，如果正当使用，大数据可以使用更多的信息帮助我们加强隐私保护，最终提高情报的质量（尤其是准确性）以识别网络空间潜在的攻击和攻击者。

例如，在理想世界中，我们不必担心欺诈邮件，因为大数据分析引擎可以精确的识别出哪些是恶意邮件。

大数据是如何用来帮助你或攻击你的

同样，大数据也存在安全隐患。例如，很多公司急于向用户投放针对性的广告并追踪你网上的每一条动向，而大数据的使用使得追踪更加简单，成本低，而且更容易分析。

例如像 IBM 公司的性格剖析服务建立的详细个人简介，比基本的人口统计资料和位置信息做的还要精确。你的网购习惯可以反映你的部分性格特征，例如你是否外向，有没有环保意识，政治是否保守或者是否喜欢去非洲旅游。

行业专家对于大数据的这种能力做了有利辩解，声称有利于改善用户的上网体验。但是我们不难想象，信息同样可能被轻易用来攻击我们。

要解决安全问题，禁止大规模数据收集是不现实的，我们应该采用最佳的方法来保护我们的隐私同时允许大数据合法使用。

驾驭大数据的关键在于数据透明，这样能够解决其面临的安全与隐私挑战。因此，大数据收集者应公开他们在收集什么信息、出于什么目的。

此外，用户必须知道数据是如何存储的，谁可以访问、访问权是如何授予的。最后，大数据公司要对它们用于安全控制方法做出具体解释以获得公众的信任。

原文名称	Big data security problems threaten consumers' privacy
作者简介	Jungwoo Ryoo，美国阿而图纳市宾夕法尼亚国立大学信息科技学院副教授，主要的研究领域有信息安全、软件工程、计算机网络。发表过多篇学术文章并对软件安全进行过广泛调研。
原文信息	2016 年 2 月 23 日发布于 The Convention，原文地址 http://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798
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.Wirenet 样本分析报告》

近日，安天追影小组在整理网络安全事件时，针对 Linux 平台下名为 Backdoor.Wirenet 的木马进行了简要分析。该木马以 Opera、Firefox、Chrome 和 Chromium 等跨平台浏览器，以及 Thunderbird、SeaMonkey 和 Pidgin 等应用的密码为目标，意图窃取用户信息。Wirenet 在 Linux 平台下会自动复制至“~/WIFIADAPT”目录，然后使用 AES 加密通道，连线至 C&C 服务器。

安天追影小组针对 Backdoor 木马家族中 MD5 为 9A0E765EECC5433AF3DC726206ECC56E 的样本进行了分析。该样本的函数数量较多，大部分的字符串信息已经被加密，其样本在网络传输过程中使用了 AES 加密。因此，样本 main 函数执行时首先进行了 AES 的初始化操作，通过进一步的分析，得出其使用的 AES 加密模式为 CFB。其次，样本 main 函数中还调用了一个 InstallHost 函数用于执行自我安装，同时在 ReadSettings 函数中包含了一些设置的重要信息。进入 ReadSettings 函数发现样本的重要信息都采用 RC4 加密方式进行加密过，通过 GDB 动态调试可获取到大量信息。如连接的服务器，密码等，这些信息在 InstallHost 函数中被使用，而 InstallHost 函数中的 Wirenet 使用解密出的信息与服务器建立连接，并且在 /.config/autostart 中设置开机自启动功能。另外样本中还有一个重要的函数 ProcessData，通过对 ProcessData 函数的调用关系可发现，该函数包含了大量功能，如遍历文件夹、读写文件、获取操作系统版本和用户信息、鼠标监控、开关机等，Wirenet 基本具备了一个普通后门程序所具备的功能。

除此之外，ProcessData 函数中有 GetGoogleChromePasswords、GetChromiumPasswords、FindMozillaLib 等函数，在这些函数中，Wirenet 会获取各浏览器安装目录下的 Passwords 文件，并连接 SQLite 尝试进行破解。

随着 Linux 操作系统的日益普遍，木马程序也开始逐渐入侵 Linux 系统。安天提醒电脑使用者要提高安全意识，定时给电脑进行体检，以确保在病毒入侵时及时发现并处理。在日常使用电脑工作时，可关闭不必要的服务。对于对外公开的服务，需要及时关注相应服务器软件的 bug 信息，并及时把软件升级到稳定版本。养成良好的备份数据习惯，当机器遭到攻击，数据不至丢失殆尽。

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、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 鉴定器、静态分析鉴定器、动态行为（默认环境）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、安全云鉴定器将文件判定为木马程序。

该文件具有以下行为：自复制、修改文件权限。

文件名	9A0E765EECC5433AF3DC726206ECC56E
文件类型	BinExecute/Linux.ELF
大小	63 KB
MD5	9A0E765EECC5433AF3DC726206ECC56E
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Wirenet
判定依据	安全云

◆ 运行环境

操作系统	中标麒麟
内置软件	默认

◆ 危险行为

行为描述	自复制
危险等级	★★★★★

◆ 其他行为

行为描述	获取系统版本
危险等级	★★

◆ 网络监控：访问 IP

IP 地址	212.7.208.65	归属地	N/A
端口	4141	域名	N/A

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=9A0E765EECC5433AF3DC726206ECC56E