安天周观察

主办：安天　　2015 年 8 月 31 日（总第 7 期）试行　本期 4 版　　微信搜索：antiylab

“首届黑龙江省互联网大会”召开 安天参加并发表主题演讲

8 月 26 日，第一届黑龙江省互联网大会在哈尔滨举行。本次大会主题为“互联网 + 龙江发展新动能”，来自政府部门、互联网企业、信息安全企业、省内传统企业及互联网创业者共 500 余人参加。

北京大学、中国信息通信研究院等单位的领导和专家献上了近 15 场有关“互联网 +”的多角度演讲和讨论。

安天技术负责人发表《APT 攻击：互联网 + 时代需要直面的安全风险》演讲指出：应全面关注网络攻击带来的纵深挑战，需要关注对手的实际能力和作业特点。同时也提出互联网 + 时代我们的安全观，更需要从治理安全观向博弈安全观、合规安全观向能力安全观、边界安全观向国土安全观的全面变革。

【安天 CERT】发布

《VBA 病毒“制造机”正在流行》报告

（第四版）

黑客组织入侵泰国 6 个政府网站

据报道，泰国 6 个政府网站在 24 日遭黑客入侵，并在网页上张贴缅甸罗兴亚族逃亡及在炸弹袭击中受害的儿童照片。6 个遭入侵的网站包括北部南奔府、中部信武里府、沙缴府、来兴府等政府网站。

黑客声称来自突尼斯黑客组织 FallagGassrini & Dr. Lamouchi，自称为伊斯兰教徒，呼吁他人尊重他们。据指，该黑客组织曾于法国《查理周刊》杂志社遭伊斯兰教枪手血洗后，入侵数个以色列及法国网站。

泰国信息及通讯科技部官员指，黑客使用 Linux 系统在全球同步发动攻击，现正调查其服务器所在地。(http://finance.chinanews.com/gj/2015/08-24/7485906.shtml)

文评

老工业基地的『互联网 +』时代

对于黑龙江这样一个老工业基地，如何能够切实落实中央提出的“互联网 +”战略，调整产业结构、转变发展方式？参加第一届黑龙江省互联网大会的嘉宾，从多种角度进行了诠释和设想。

由于黑龙江的历史和现状，决定了针对黑龙江的“互联网 +”战略，最重要的是加快解决工业互联网的建设问题。“互联网 + 工业”的创新发展并不仅仅需要基础设施的建设的保障，实际上，针对新型工业技术理论、框架、关键技术等仔细分析，会发现对网络安全防护工作提出了更高的要求，安全应当是“互联网 +”工业发展的前提保障。

互联网 + 的快速推进增大了上位机暴露和被攻击的可能性，2010 年 Stuxnet（震网）病毒的发生让人们初识 APT 攻击对于工业系统造成的巨大威胁。随着网络安全威胁正在向传统领域延伸，亦随同智能设备的发展泛化，互联网 + 在拉动传统领域和行业加速发展的同时，也在加速着网络安全威胁和传统领域风险的合流，增加了 APT 攻击（高级持续性威胁）的攻击面，亦增加了网络犯罪的获利空间。所以，对于工业控制系统的安全问题，首先要把工控风险防御放置于工控体系之前。

对于期待通过“互联网 +”加快老工业基地创新发展的黑龙江来说，“互联网 +”改变了人们的生活方式、生产方式、工作方式，而如果没有网络安全的保护，将会危及到我们赖以生存的真实世界。

每周安全事件

类 型	内 容
中文标题	GitHub 遭受 DDoS 攻击
英文标题	GitHub wobbles under DDoS attack
作者及单位	Simon Sharwood，The Register
内容概述	GitHub 遭不明攻击者的 DDoS 攻击。GitHub 状态页面在周二显示“容量过载”，同时对网站服务器进行了攻击。截止到目前，该网站的所有服务暂时恢复正常。这是 GitHub 在 2015 年遭受的第二次 DDoS 攻击。
链接地址	http://www.theregister.co.uk/2015/08/26/github_wobbles_under_ddos_attack/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 2 个移动平台和 12 个 pc 平台的恶意代码家族值得关注

病毒分类	病毒名称	病毒特点
移动恶意代码	GrayWare[AdWare]/AndroidOS.Callflakes 发现日期：2015.8.22	一类推广应用的灰色软件家族。该家族样本可以连接网络下载，在用户手机中安装不需要的应用程序，威胁较低。
	Trojan[Downloader]/AndroidOS.Guerrilla 发现日期：2015.8.23	一类基于安卓系统的木马家族。该家族样本可以下载其他应用或恶意代码，还可以拦截用户短信，有一定威胁。
PC 恶意代码	Trojan[Downloader]/MSIL.Injector 发现日期：2015.8.21	一类可以注入系统进程并下载其他恶意代码的木马家族。可以隐藏自身，威胁较高。
	Trojan[Banker]/Win3 2.BitClip 发现日期：2015.8.21	一类可以窃取比特币账户相关信息的木马家族。该家族样本运行后获取剪贴板的内容并回传，威胁较高。
	Trojan[Backdoor]/Win32.Emdivi 发现日期：2015.8.21	一类 APT 相关的木马家族。该家族样本属于名为“蓝白蚁”的针对日本的 APT 行动，是一个拥有多种指令的后门，威胁极大。
	Trojan/Win32.Polbogri 发现日期：2015.8.21	一类可以窃取用户信息的木马家族。该家族样本可以下载其他恶意代码并安装，窃取用户敏感信息、修改文件等。
	GrayWare[AdWare]/JS.Dealpeak 发现日期：2015.8.21	一类下载推广应用并安装的灰色软件家族。该家族样本下载并安装用户不想使用的应用程序，威胁较低。
	Trojan[Banker]/Win32.Bradelf 发现日期：2015.8.22	一类盗取银行账号的木马家族。它可以收集用户系统信息并回传给攻击者，威胁较高。
	Trojan/Win32.GreenShaitan 发现日期：2015.8.22	一类可以窃取用户信息的木马家族。该家族样本可以连接远程服务器接受恶意操作，有一定威胁。
	Trojan/Win32.Chevalka 发现日期：2015.8.22	一类可以窃取用户文档的木马家族。该家族样本能遍历磁盘文件，查找文档及表格后缀的文件并回传，威胁较高。
	RiskWare[WebToolbar]/Win32.DfltTab 发现日期：2015.8.22	一类安装浏览器插件的风险软件家族。该家族样本为浏览器安装插件，更改主页、搜索引擎及标签页的设置，搜索时会弹出广告，威胁较低。
	RiskWare[WebToolbar]/JS.AgentBar 发现日期：2015.8.22	一类利用 JS 脚本编写的安装浏览器插件的风险软件家族。用浏览器时弹出广告，威胁较低。
	RiskWare[Server-Web]/Win32.Agent 发现日期：2015.8.22	一类改变用户浏览器默认搜索引擎的风险软件家族。它改变默认搜索引擎为 CouponsBar 搜索引擎，会弹出广告，威胁较低。
	HackTool[Hoax]/Win32.RegistryCleaner 发现日期：2015.8.22	一类可以对注册表进行清理的黑客工具家族。该家族样本可以对用户系统的注册表进行清理，但实际作用并不大。

NSA 和 AT&T 间谍条约知多少

Kim Zetter / 文　　安天公益翻译小组 / 译

8 月 15 日，《纽约时报》发布了一份最新的斯诺登文件，该文件揭示了 NSA(美国国家安全局) 和 AT&T 公司长达 10 年的秘密合作伙伴关系，AT&T 向 NSA 提供了数十亿电子邮件的元数据。《纽约时报》的报道引发了大量关注，但文章没有详细介绍 AT&T 公司是如何为 NSA 虹吸数据和执行间谍活动的。

在斯诺登文件中，并没有明确点名 AT&T 公司，但是《纽约时报》指出，“大量证据”显示 AT&T 是文件中提到的主要公司，一些情报官员已经证实了这一点。

《连线杂志》和《沙龙杂志》在近 10 年内发布的报道里详细介绍了 AT&T 设在旧金山、密苏里州和美国其他地区的“秘密房间”，并指出 NSA 就利用这些房间来虹吸互联网数据。一些媒体在 2006 年披露过 NSA 和 AT&T 公司合作关系，当时在旧金山任职的前 AT&T 技术人员马克·克莱恩和另外两名在其他地区任职的前 AT&T 技术人员提供了 AT&T 在布里奇顿、密苏里州和旧金山设立的秘密房间的信息。

据他们说，2002 年，AT&T 首先在布里奇顿建成了高度安全的房间，AT&T 为房间装备了生物识别的“屏障”，用视网膜和指纹扫描仪进行保护，只有具备 TS/SCI(绝密 / 机密) 安全许可的工作人员才被允许进入。当地工作人员被告知，该房间用于为政府机构监视网络流量。

该布里奇顿设施是 NSA 获取数据的重要设施，因为它是 AT&T 的技术指挥中心。在这里 AT&T 管理着所有承载其国内和国际互联网流量的路由器和线路，当时，

设在马里兰州米德堡的 NSA 总部

AT&T 控制着美国家庭和企业互联网流量约三分之一的带宽，这相当于给了 NSA 访问大规模数据的权限。

而布里奇顿房间并不是唯一的 AT&T 为 NSA 设立的秘密房间，AT&T 还在美国其他几个城市设立了秘密房间。《纽约时报》获得的斯诺登文件显示，该公司至少在它的 17 个互联网枢纽安装了监控设备。虽然没有具体说明是哪些城市，但从《连线杂志》2006 年获得的文件显示，除了旧金山和布里奇顿，AT&T 还在西雅图、圣何塞、洛杉矶和圣地亚哥设立了秘密房间。“这些秘密房间的装置使政府能够查看互联网上的每一条信息并分析人们在做什么”，《连线杂志》在 2006 年写道。

在 2006 年克莱因提供给《连线杂志》的文件中，详细介绍了 AT&T 如何设立这些装置。位于旧金山福尔瑟姆街的 AT&T 工厂的房间 641A 连接上了高速光纤线路，而这些线路连接到 AT&T 的 WorldNet 服务 (互联网的共同骨干网的一部分) 路由器，只有具备安全许可的 NSA 管理层技术人员能够进入房间。

2002 年拟定的密室计划讨论了窥探光纤电路的困难性。发射电磁场的铜线线路能够在不干扰线路的情况下进行窃听，与此不同，光纤线路不会泄露光信号。为了监控光纤线路的通信，技术人员必须物理性地切断线路，用分配器转移光信号，从而虹吸数据。AT&T 将信号转移到秘密房间中的一个特殊设备中，由 Narus 公司生产的设备会分析流量并过滤，从而向 NSA 提供它想要的数据，这包括赋予 NSA 访问数十亿电子邮件元数据的权限。

根据《纽约时报》报道，在代号为“Fairview”的项目中，AT&T 从 2001 年 10 月就开始向 NSA 提交电子邮件和其它互联网数据，这是发生在秘密房间建成之前。在该项目中，AT&T 向位于马里兰州米德堡的 NSA 总部转发了 4000 亿互联网元数据，其中包括电子邮件发件人和接收人等细节信息，但是不包括信件的内容。AT&T 每天向 NSA 转发超过 100 万的电子邮件，NSA 关键字选择系统会对这些邮件进行过滤。2003 年 9 月，AT&T 为 NSA 启用了新的收集能力，使其能够实时了解全球网络中的信息。2011 年，AT&T 开始向 NSA 提供手机元数据，包括每天 11 亿国内手机通话记录。

斯诺登 2013 年泄露的文件为克莱因和另外两位匿名 AT&T 技术人员在 2006 年的说法提供了鲜明的证据。但是目前还不清楚，虹吸互联网数据的项目是否还与其初始形式相同。在过去的两年里，各种披露显示了 NSA 监控项目的广泛性，也曝光了 NSA 与科技企业的合作关系，这迫使 NSA 不得不削减这样的一些监控活动。在公众愤怒抗议之后，一些公司也开始拒绝 NSA 获取数据的请求。

原文名称	What We Know About the NSA and AT&T's Spying Pact
作者简介	Kim Zetter，《连线杂志》一位屡获殊荣的资深记者，研究范围包括网络犯罪、隐私和安全。
原文信息	2015 年 8 月 17 日发布于《连线杂志》，原文地址 http://www.wired.com/2015/08/know-nsa-atts-spying-pact/

【安天 CERT】发布

《VBA 病毒“制造机”正在流行》报告

最近，安天 CERT(安全研究与应急处理中心)的安全研究人员发现了一个用于生成宏病毒的生成器。生成器根据用户配置可以生成在微软 Word 和 Excel 执行的恶意宏文件。生成器采取 .net 平台编写，用大量混淆方法和加密措施来进行反逆向行为。而生成器生成的宏病毒代码同样采取了混淆函数名和加密函数参数等方式来反杀毒软件。经证明其反杀毒能力很强，几乎目前所有产品均无法检测。生成器内置加密器具备加密恶意软件、配置恶意软件自动运行、静默运行等多种功能。而后经过大量分析发现目前多数宏病毒都由生成器生成伴随邮件肆虐传播。

宏病毒十分猖獗，在安天 CERT 捕获了大量宏病毒的基础上，经过分析推断他们其中绝大部分都是由生成器生成。而生成器的特点是，大部分源码的框架与内部加密算法一致，唯有一些配置不同，最典型的是内嵌的加密 URL 不同。在报告中，通过两个案例分析来揭示了其他生成器的工作方式。

安天 CERT 的研究人员指出，如今生成器正在流行，且宏病毒散布广泛，伴随着其他技术死灰复燃，宏病毒嵌入地址可以是正常网站被“挂马”的恶意样本、黑服务器的样本、亦或是 APT 样本。并且这种传播方式多数为邮件传播。目前主机、服务器安全的加固、防火墙的严格守护，使得邮件传播是个绝佳的入口，而且利用文档进行传播不容易引起用户怀疑，且传播便捷，成功率高。这些特点正在逐步演变为默认的传播方式。用户要提高警惕，不要下载来历不明的邮件附件，更要谨慎点击文档的“启用宏”功能，目前良性使用宏的文档已不多见，而更多的是把文档作为跳板利用宏作为感染机器的“杀手”。针对该恶意程序，安天追影高级威胁鉴定系统无需升级即可有效检测，引擎更新库后已经可以实现有效检测。

(报告原文：http://www.antiy.com/response/Builderexp.html)

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，即可实现对上述宏病毒进行有效检测，下为其自动形成的分析报告

该恶意程序由安天威胁检测系统发现，经过追影威胁分析系统分析。经由 BD 静态分析鉴定器、美国软件交叉索引(NSRL)鉴定器、数字证书鉴定器、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、智能学习鉴定器、安全云鉴定器等鉴定分析。

依据 BD 静态分析鉴定器最终将文件判定为木马程序。

该文件具有以下行为：获取系统版本；创建互斥体(mutex)；隐藏文件；连接网络；获取计算机名称；创建特定窗体；获取 socket 本地名称；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；请求加载驱动的权限；获取主机用户名称。

文件名	Название.doc
文件类型	Document/Microsoft.DOC[:Word 97−2003]
大小	262 KB
MD5	BECF0D27E48BB7A160E69A177189D03E
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Downloader]/MSWord.Agent.qw
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=BECF0D27E48BB7A160E69A177189D03E

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取系统版本	★	创建互斥体 (mutex)	★
隐藏文件	★★	连接网络	★
获取计算机名称	★	获取 socket 本地名称	★
创建特定窗体	★	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		请求加载驱动的权限	
获取主机用户名称			