安天周观察

主办：安天　2016 年 8 月 1 日（总第 50 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加 2016 中国互联网企业社会责任论坛并发言

7 月 26 日，由国家网信办网络社会工作局、工业和信息化部信息通信管理局指导，中国互联网协会主办的 2016（第三届）中国互联网企业社会责任论坛在北京召开。本届论坛旨在倡导互联网企业学习贯彻习近平总书记“4·19”网信座谈会重要讲话精神，积极履行社会责任，共建网络强国。

在大会设立的分论坛上，安天、阿里巴巴、腾讯、启明星辰等企业代表就“网络安全与企业社会责任”这个话题展开了圆桌交流。安天副总经理赵焕菊在发言中围绕“不忘初心，继续前行，履行责任，担当使命”的主题，汇报了安天 16 年来在技术创新、产品实现、应急响应、沟通协作方面的成绩。她表示，安天始终站在应对网络威胁的第一线，致力于提供先进的威胁检测能力，围绕企业的社会责任来构建企业发展的基业。秉承“服务客户，解决问题，应对威胁，保障价值”的原则，以技术创新和产品实现来构建安全基础能力，以应急响应和安保活动来确保实施应对威胁，积极参与业界沟通与协作，促进技术发展与分享，为国家网络安全与行业发展建言献策。最后，她说道：“维护国家网络安全，构建健康网络空间，是网络安全企业应尽的社会责任，也是时代赋予我们的历史使命。安天愿意与大家一起，不忘初心，继续前行，履行责任，担当使命。”

大量无线键盘存在可嗅探用户输入的 KeySniffer 漏洞

近日，研究人员发现了一种名为“KeySniffer”的无线键盘漏洞，其不需要匹配设备，就能够让黑客获取到无线键盘和 USB 适配器传输的数据，包括用户名、密码、信用卡等任何使用无线键盘输入的信息。

存在漏洞的键盘与插入电脑的 USB 无线接收器之间的数据都是明文传输的。由于没有加密，攻击者还能够在数据流中注入他们自己的键盘敲击。黑客如果想要注入恶意的键盘输入，可以通过脚本自动化执行。唯一的条件就是等待用户离开电脑几分钟。很多操作系统在鼠标操作失灵时会提供基于键盘的控制，因此，控制了用户的键盘就相当于控制了整台电脑。（文章来源：http://news.softpedia.com/news/keysniffer-flaw-lets-attackers-log-and-inject-keystrokes-on-wireless-keyboards-506642.shtml）

一周简讯

- 研究人员发布勒索软件 Bart 及 PowerWare 解密工具
- PHP 0day 漏洞，允许攻击者以上帝模式访问网站
- 研究人员发现 Hackhound 及其 C2 被用于工业间谍活动
- 安天 AVL 联合猎豹曝光仿冒知名游戏手机病毒
- 研究人员破解 Mad Max 僵尸网络混淆域名生成算法
- 研究人员曝光利用亚马逊隐藏订单功能的新型钓鱼骗术
- 研究人员发现勒索软件 Petya 和 Mischa 以服务形式出现

（安天 CERT 搜集整理，详见：http://bbs.antiy.cn）

安天在“2016 年俄语国家网络空间安全管理与保障研修班”结业仪式上发表演讲

近日，由中华人民共和国商务部、中华人民共和国国家互联网信息办公室主办的“2016 年俄语国家网络空间安全管理与保障研修班”在北京圆满落幕。

在研修班结业仪式上，来自安天安全研究与应急处理中心的恶意代码分析工程师白淳升，为学员们带来了题为《APT 分享技术及案例研究》的演讲，他主要介绍了一些 APT 事件分析技术，如鱼叉式钓鱼邮件、水坑攻击、样本关联分析的方法，并结合白象事件等几起 APT 攻击事件举例了 APT 溯源、定位的一些技术手段。同时，他表示目前的一些 APT 攻击仍会使用一些公开漏洞和通用恶意代码，这体现了国内现阶段网络安全意识普遍薄弱的现状，意味着网络空间基础安全能力的提升迫在眉睫。最后，他在总结中说道：“网络空间防御能力最终会由攻击者和窥视者来检验，APT 防御需要信息化基本环节和安全能力的共同完善，而反 APT 则是一种综合的体系的较量。”

每周安全事件

类 型	内 容
中文标题	思科公司的数据中心运营管理解决方案中存在严重漏洞
英文标题	Cisco plugs critical flaw in data center operations management solution
作者及单位	Zeljka Zorz；Help Net Security
内容概述	近日，安全研究专家在思科统一计算系统 (UCS) 的性能管理软件中发现了一个严重的安全漏洞。这个严重的安全漏洞存在于软件的 web 框架中。当用户通过 HTTP 的 GET 请求向服务器传递输入数据时，系统会对输入参数进行验证。当验证失败时，这个漏洞将会被触发。攻击者只需要向受此漏洞影响的系统发送特制的 HTTP GET 请求，就可以利用这一漏洞来对目标进行攻击。一旦攻击者成功利用了这个漏洞，他就可以获取到目标主机的 root 用户权限，并在主机中执行任意的控制命令。目前，思科公司已经修复了这一漏洞，并建议系统管理员尽快将软件的版本更新至 2.0.1。
链接地址	https://www.helpnetsecurity.com/2016/07/21/data-center-operations-cisco/?utm_source=dlvr.it&utm_medium=twitter

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 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.FakeSystem.c[exp]2016-07-25	该应用程序运行后会联网获取配置信息，根据指令进行下载安装未知文件，自动回复短信，执行通知栏推送等行为，建议立即卸载，避免造成资费损耗。（威胁等级高）
		Trojan/Android.Mobilespy.s[prv，spy]2016-07-26	该应用是一款间谍软件，安装后需要设置上传邮箱地址信息，运行后会上传手机联系人信息和短信箱内容，会造成用户隐私泄露和资费消耗，如非本人安装建议及时卸载该程序。（威胁等级中）
		Trojan/Android.Sadstrot.b[rmt，prv]2016-07-27	该应用安装无图标，运行时会获取用户短信箱、联系人、通话记录等隐私信息，并联网上传，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.Omni.c[prv，rmt]2016-07-28	该应用运行后会加载资源文件，生成恶意 apk 应用并安装，会在后台私自拦截用户短信，上传用户短信，联网上传用户设备信息，获取指令，获取设备上运行的服务和进程，查看和删除浏览历史记录，拨打电话或发送短信记录音频等其他的命令，会造成用户隐私泄露。（威胁等级中）
	较为活跃的样本	Trojan/Android.E4AQQspy.i[prv]	该应用伪装成 QQ 刷钻工具，运行时会后台上传通话记录和通讯录，造成隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.FakeFlashPlayer.o[exp，prv]	该应用伪装成 Adobe Flash Player，运行后隐藏图标，窃取设备固件信息，私自联网获取指令，下载恶意数据或上传本地文件，建议用户立即卸载。（威胁等级高）
		Trojan/Android.Downloader.cb[rog，exp]	该应用程序伪装成系统应用，安装无图标，运行后联网获取下载相关参数数据，私自下载 APP 并安装到系统应用里面，造成用户资费消耗。（威胁等级中）
		Trojan/Android.SmsThief.ak[prv，exp]	该应用伪装成 google 应用，运行后隐藏图标，窃取手机短信和相关信息，并将获取的短信和手机信息转发到指定 url，造成用户隐私泄露和资费消耗。（威胁等级中）
		Trojan/Android.jianmo.an[rog，sys]	该应用程序伪装成 QQ，运行后诱导激活设备管理器，显示虚假登陆界面，上传用户社交账号密码信息，获取设备锁屏密码进入勒索界面，造成用户隐私泄露，影响用户正常用机体验，建议卸载该程序。（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 Windows 打印后台处理程序远程执行代码漏洞 CVE-2016-3238	Microsoft Windows 是美国微软 (Microsoft) 公司发布的一系列操作系统。Print Spooler service 是其中的一个打印服务组件。 Microsoft Windows Print Spooler 存在远程执行代码漏洞，该漏洞源于服务器在安装打印机的过程中，打印后台处理程序服务未正确地验证打印驱动程序。攻击者可利用该漏洞执行任意代码，还可以控制受影响的系统。（威胁等级高）
	较为活跃的样本	Trojan[Backdoor]/Win32.Dridex	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后可以连接远程服务器，攻击者可以进行各种操作，收集用户的敏感信息。（威胁等级中）
		RiskWare[Downloader]/Win32.Trick	此威胁是一类可以下载广告应用的灰色软件家族。该家族样本运行后可以连接网络下载广告软件并安装，占用系统资源，影响用户使用。（威胁等级中）
		Trojan[Downloader]/Win32.Nurjax	此威胁是一类可以下载恶意代码的木马家族。该家族样本运行后可以劫持浏览器，在用户浏览特定网页时重定向到恶意页面，下载恶意代码并运行。（威胁等级中）
		GrayWare[AdWare]/NSIS.Gavady	此威胁是一类可以下载并安装推广应用的灰色软件家族。该家族样本运行后会连接网络，下载并安装名为“FLV Player”的推广应用，占用系统资源，影响用户使用。（威胁等级高）

NIST 建议停止使用短信双因素认证

Chris Brook / 文　安天公益翻译小组 / 译

近日，一个美国政府机构表示，基于短信的双因素认证濒临末日，理由是该功能缺乏安全性。

美国国家标准技术研究所 (NIST) 发布的《数字认证指南》最新版草案指出，该方法将很快会被弃用。《数字认证指南》规定了所有认证软件最终需遵循的规则。NIST 在其中指出短信存在被截获或重定向的风险，其鼓励任何考虑采用双因素认证的服务，可以尝试一下替代的认证方法。

在该指南中，NIST 称，服务需要确认它发送代码的电话号码属于合法的网络，而不是一个 VoIP 服务 (Voice over Internet Protocol 网络电话，简而言之就是将模拟信号数字化，以数据封包的形式在 IP 网络上做实时传递)。

“如果使用公用移动电话网络上的短信进行带外验证，验证者应验证正在使用的预注册电话号码真的与移动网络而非 VoIP(或其他基于软件的) 服务相关。”

该指南写到：“如果不进行双因素认证，就应无法更改预注册的电话号码。使用短信的带外数据 (OOB) 已被弃用，在该指南的未来版本中可能还会被禁止。”

同时，NIST 称，该文件确实支持生物识别技术 (即使其使用受到限制) 进行身份验证。虽然生物识别技术认证本身可能会出现误匹配率，可能会被欺骗，无法为验证者提供明确的结论，但是只要是生物识别技术与另一种身份验证因素一起使用，其就会被允许。

NIST 强调该文件目前还处于公开预览阶段，这意味着，其中的流程尚未落实，仍然接受公众的意见。NIST 将在大约两周的时间里收集意见，之后编辑人员会用 2–3 周的时间审查这些意见。

该机构通过 GitHub 来寻求公众对 SP 800–63–3 的意见。NIST 说，虽然该平台看起来可能不那么正统，但是它认为该网站是一个强大的文件起草论坛，会鼓励公众踊跃地提出技术和程序方面的意见。近期，NIST 首次呼吁公众协助其制订该指南，并将该指南上传至 GitHub 网站。

目前，一些服务已经开始弃用双因素认证。脸书开始使用代码生成器 (Code Generator) 作为其登录认证功能的一部分。当用户登录时，打开该代码生成器，会被要求输入特殊的安全代码，而该代码每 30 秒改变一次。谷歌也有类似的功能——谷歌身份验证器 (Google Authenticator)，它为用户提供 6 到 8 位数的一次性密码。其他公司，如 Authy 和 Duo，也有特殊的解决方案。

在过去的几年中，双因素认证几乎已经无处不在。该功能允许服务向用户发送一个代码，用户使用该代码和自己的密码来进入服务。它作为一种附加的安全层的功能，已经被多个行业采用。一些公司，如 Apple，Dropbox，Snapchat，Evernote 和 Twitter，都采用了双因素身份认证，以对抗账户接管和感染。

尽管如此，双因素认证并非“银子弹”，攻击者和研究人员都发现了该方法的漏洞，主要是通过中间人攻击。两年前，Duo 的研究人员发现了一种方法来绕过贝宝使用的机制，将受害者账户中的资金转给他们选择的任何收款人。WordPress、Google 和 Instagram 提供的插件也出现了漏洞，允许黑客绕过双因素认证。

原文名称	NIST Recommends SMS Two-Factor Authentication Deprecation
作者简介	Chris Brook，Threatpost 副编辑。
原文信息	2016 年 7 月 27 日 Threatpost 发布 原文地址 https://threatpost.com/nist-recommends-sms-two-factor-authentication-deprecation/119507/
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
《白象的舞步——来自南亚次大陆的网络攻击（二）》

近日，安天发布了名为《白象的舞步——来自南亚次大陆的网络攻击》的分析报告，披露了两组针对我国多领域的高频度APT攻击事件。在上一期的《安天周观察》中，追影小组分析了2012--2013年间捕获的攻击波——“白象一代”。本期我们将继续研究“白象行动”中的第二波攻击——2015年年底被捕获的“白象二代”。

1.“白象二代”概况

“白象二代”摆脱了“白象一代”杂乱无章的攻击手法，整体攻击行动显得更加正规化和流程化。其普遍使用了具有极高社工构造技巧的鱼叉式钓鱼邮件进行定向投放；至少使用了CVE-2014-4114和CVE-2015-1641等三个漏洞；其在传播层上不再单纯采用附件而转为下载链接，部分漏洞利用采取了反检测技术对抗；其相关载荷的HASH数量则明显减少，使用了通过Autoit脚本语言和疑似由商业攻击平台MSF生成的ShellCode；同时初步具备了更为清晰的远程控制指令体系。

2. 样本行为

hash为F0D9616065D96CFCBB614CE99DD8AD86的样本分析：

1) 该样本主要利用CVE-2014-4114漏洞进行攻击。

2) CVE-2014-4114是OLE包管理INF任意代码执行漏洞，该漏洞影响Win Vista、Win7等以上操作系统，攻击者使用PowerPoint作为攻击载体，该漏洞是在Microsoft Windows和服务器上的OLE包管理器。在OLE打包文件(packer.dll)中能够下载并执行类似的INF外部文件，允许攻击者执行命令。

3) 白象攻击使用的PPS扩展名样本利用Windows OLE远程代码执行漏洞CVE-2014-4114释放并执行可执行文件。值得注意的是，在此前分析过的其他攻击组织使用的4114样本中，多数为Office高版本格式，主要是一个以XML为索引的压缩包，其内嵌的PE载荷会被杀毒软件在解压递归中检测到，但这次“白象二代”组织使用了低版本Office的传统LAOLA格式，由于对安全厂商来说这是一个“未公开格式”，所以其达到了一定的免杀效果。

目前，安天追影威胁分析系统已经可以对“白象行动”的相关样本进行检出，并会持续提升对未知威胁的检测能力。（完整报告：http://www.antiy.com/response/WhiteElephant/WhiteElephant.html）

高级威胁 安天【追影威胁分析系统】无需更新病毒库，即可实现对上述高级威胁进行有效检测，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、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。

最终依据静态分析鉴定器、动态行为鉴定器将文件判定为高级威胁。该文件具有以下行为：格式漏洞、获取系统版本、获取主机用户名称、查找指定内核模块、隐藏文件、查找特定窗体、请求加载驱动的权限、创建特定窗体、获取驱动器类型、获取系统内存、打开自身进程文件、独占打开文件、获取计算机名称、疑似桌面控制。

同时，该文件利用了CVE-2014-4114漏洞。

文件名	F0D9616065D96CFCBB614CE99DD8AD86
文件类型	Document/Microsoft.PPT[:PowerPoint 98-2003]
大小	12.21 MB
MD5	F0D9616065D96CFCBB614CE99DD8AD86
病毒类型	高级威胁
恶意判定/病毒名称	Trojan[Exploit]/Win32.CVE-2014-4114
判定依据	静态分析

◆ 漏洞信息

编号	CVE-2014-4114		
首次发布	2014-10-15	最后更新	2014-11-17
描述	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object in an Office document, as exploited in the wild with a "Sandworm" attack in June through October 2014, aka "Windows OLE Remote Code Execution Vulnerability."		

◆ 危险行为

行为描述	危险等级
格式漏洞	★★★★

◆ 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	★★	获取主机用户名称	★
查找指定内核模块	★	隐藏文件	★
查找特定窗体	★	请求加载驱动的权限	★
创建特定窗体	★	获取驱动器类型	★
获取系统内存	★★	打开自身进程文件	★
独占打开文件	★	获取计算机名称	★
疑似桌面控制	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=F0D9616065D96CFCBB614CE99DD8AD86