安天周观察

主办：安天　2016 年 11 月 14 日（总第 64 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 年古巴国家信息化发展战略与规划官员研修班

11 月 3 日 -17 日，由国家商务部和国家互联网信息办公室主办的“2016 年古巴国家信息化发展战略与规划官员研修班”在北京举办，共有来自古巴的互联网领域官员 40 余名学员参加培训。

在 11 月 8 日的培训中，安天派出在安全研究和应急响应方面具有丰富经验的工程师担任本次培训的讲师，为学员们带来了题为《中国面临的 APT 攻击风险和案例分析》的演讲。

首先，安天讲师分析了中国所面临的网络安全形势以及层出不穷的 APT 攻击所带有的政治经济背景，重点介绍了各种不同攻击能力水平的 APT 攻击案例以及安天所提出的防御系统和新的布防点。并表示当前的 APT 攻击已经表现出一定的针对性和多样性，传统的安全环节已渐渐不能满足安全需求，所以需要设置新的防御系统和布防点。

随后，安天讲师提出的布防点包括：使用传统安全手段前置过滤一般性威胁；凭借静态检测能力过滤已知恶意代码，并为高价值威胁的定性提供参考依据；基于前置沙箱技术，增加 0day 发现能力，并及时发现未知的恶意代码，结合已有的白名单和安全基线策略的终端防御，有效组织威胁入侵，降低在终端的攻击成功率。同时，不同设备和系统之间存在联动机制，可构建高纵深，多层次的综合防御体系。使 APT 攻击能够被有效防御；即使防御失败，也能尽早发现；即使未能及时发现，也可以及时补救，防止敏感信息泄露，阻断攻击者的远程控制通道。

安天讲师的精彩演讲和专业视角得到了与会古巴信息官员的高度重视与认可。

一直以来，安天始终站在应对网络威胁的第一线，积极参与国际安全产业沟通与协作。从“中国 – 东盟信息港论坛：网络安全”闭门会议，到“俄语国家网络空间安全管理与保障研修班”和“阿拉伯国家网络空间安全管理与保障研修班”，再到“2016 年古巴国家信息化发展战略与规划官员研修班”，各类国际培训会议都能听到安天为网络安全与行业发展建言献策的声音。

■ 黑客可利用 4G LTE 协议中断移动设备网络

近日，研究人员在 2016 欧洲黑帽大会上通过演示证明，4G LTE 协议容易被黑客攻击。研究人员在测试网络上模拟实验：从芬兰对不具名的英国移动运营商发起攻击。该研究小组发现，可以通过不同的方式利用 Diameter 框架中断特定用户和节点的连接。该实验证明，能成功发起拒绝服务攻击。Diameter 正取代传统的 SS7 协议。SS7 协议自 1975 年开始使用。诺基亚贝尔实验室的安全研究人员发现，随着 4G LTE 网络的使用激增，移动运营商用 Diameter 取代 SS7。虽然大家都知道 Diameter 比 SS7 要安全，但未部署附加安全措施的情况下，Diameter 也会面临同样的网络攻击。(https://www.easyaq.com/newsdetail/id/1749765207.shtml)

■ 英国乐购网上银行近万账户遭窃，现已暂停服务

近日，英国乐购银有 40000 个网上银行账户被攻破，其中一半的账户中的钱被窃走。目前银行方面已经宣称将全额赔付被窃用户的损失。这家乐购网上银行共有超过 700 万名用户，此次事故发生后，银行方面决定暂停网络转账和支付功能直至事件得到解决，但智能卡付款系统和 ATM 机未受影响。银行账户失窃的原因目前还不得而知，乐购银行方面也没有对此作任何声明，只是回复称将赔偿用户的全部损失。(https://www.easyaq.com/newsdetail/id/268991147.shtml)

■ 新型 DDoS 攻击：利用 LDAP 服务器实现攻击放大

近日，据安全公司披露，发现一种新型 DDoS 攻击媒介针对其客户发起攻击。这种攻击技术是一种利用轻量目录访问协议 (Lightweight Directory Access Protocol，LDAP) 的放大攻击，峰值可以达到 Tb 级别。LDAP 是访问类似 Active Directory 数据库用户名和密码使用最广泛的协议。它是基于 X.500 标准的，但是简单多了并且可以根据需要定制。与 X.500 不同，LDAP 支持 TCP/IP，这对访问 Internet 是必须的。(http://www.freebuf.com/vuls/118337.html)

一周简讯

- 研究人员警告：D-Link 路由器存在 RCE 漏洞
- 安全厂商警告勒索软件 Cerber 开始加密数据库
- Bopup 商用通讯服务器存在远程代码执行漏洞
- 安全研究员发现 Gmail 严重漏洞，可轻易破解
- 新型邮件钓鱼活动针对 LinkedIn 用户
- 安全厂商分析仿冒流行应用移动木马

（安天 CERT 搜集整理，详见：http://bbs.antiy.cn）

每周安全事件

类 型	内 容
中文标题	OAuth2.0 部署不当，数十亿 Android App 账户存泄露风险
英文标题	Over 1 Billion Mobile App Accounts can be Hijacked Remotely with this Simple Hack
作者及单位	Swati Khandelwal；Thehackernews
内容概述	近日，研究人员发现，众多支持单点登录的 App 没有正确部署 OAuth2.0 认证协议，攻击者可利用此漏洞远程登陆任何用户的 App 账户。研究人员发现，许多 AndroidApp 的开发者并没有正确地核对 ID 提供方发来的信息的有效性。这些第三方 App 并没有验证访问 token，以核查用户与 ID 提供方是否关联，第三方 App 服务器只检查了这个信息是否由一个有效的 ID 提供方发出。这种部署给了攻击者可乘之机，他们可以下载存在此漏洞的 App，使用自己的信息登录，通过建立服务器，修改 ID 提供方发送的数据，将自己的用户名改为目标对象的用户名。攻击者可以利用这种方法，泄露用户敏感信息，或者以用户名义在相应 App 上操作。 研究人员发现有 OAuth 部署问题的各类 App 总共有 24 亿的下载量，专家估计将有 10 亿不同的手机 App 账户可能被劫持。
链接地址	http://thehackernews.com/2016/11/android-oauth-hacking.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.MTKbill.a[pay, prv]2016-11-07	该应用程序为测试应用，运行后会监听拦截短信，上传短信获取返回 SP 号码，会私自发送短信，用于订购付费内容，并造成用户资费损失，建议不要安装。（威胁等级高）
		Trojan/Android.x200portal.a[rmt, prv, spy]2016-11-07	该程序运行后会获取 root 权限，会激活设备管理器并隐藏图标，后台会接收短信和远程指令，执行拍照、录像等操作；会监听用户手机数据，会上传用户短信、手机固件信息、联系人列表、社交应用等隐私信息，会造成用户隐私泄露和资费损耗，请立即卸载。（威胁等级高）
		Trojan/Android.kktools.a[rmt, exp]2016-11-07	该应用会伪装为正常应用，运行后会隐藏图标，接收远程服务器指令，会私自发送扣费短信，并拦截回执短信。建议卸载，避免资费消耗。（威胁等级中）
		Trojan/Android.GPSSpy.j[prv, exp]2016-11-08	该应用无实际功能，运行后会拦截特定短信并通过短信窃取用户地理位置信息，会造成用户隐私泄露和资费损耗，建议不要安装。（威胁等级高）
	较为活跃的样本	Trojan/Android.InfoStealer.aa[prv, rmt]	该程序运行后，会收集用户短信、联系记录、浏览器搜索记录和书签、邮件信息等并且会发送给控制端，会造成隐私泄露，谨慎使用。（威胁等级中）
		Trojan/Android.SmsSend.kt[exp]	该应用运行后会私自发送指定短信，造成用户资费消耗。（威胁等级高）
		Trojan/Android.Koler.f[rog, sys]	该程序会伪装成色情播放器，运行后会激活设备管理器，隐藏图标，以非法浏览色情为由置顶界面勒索用户付费，同时会上传手机固件信息，造成用户资费损失，请不要安装。（威胁等级中）
		RiskWare/Android.Downloader.cn[rog, exp]	该应用无实际功能，包含风险下载和静默安装代码，会造成用户资费损耗，建议不要安装。（威胁等级低）
		G-Ware/Android.FakeApp.bt[exp, rog]	该程序会伪装成其他应用，无实际功能，运行后会联网获取敏感内容，并传播色情网站，会诱导用户下载其他未 apk 应用，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	Adobe Reader/Acrobat 内存破坏漏洞 (CVE-2016-6996)	Adobe Reader 是 PDF 文档阅读软件。Acrobat 是 PDF 文档编辑软件。 Adobe Reader/Acrobat < 11.0.18，Acrobat/Acrobat Reader DC Classic < 15.006.30243，Acrobat/Acrobat Reader DC Continuous < 15.020.20039 (Windows/OS X) 存在内存破坏漏洞，远程攻击者会利用此漏洞可执行任意代码或造成拒绝服务。（威胁等级高）
	较为活跃的样本	Trojan[Spy]/Win32.Crimson	此威胁是一种可以监视用户系统的木马家族。该家族样本运行后会连接远程服务器接受攻击者的监视，攻击者可以执行恶意操作，如浏览文件、上传数据等。（威胁等级中）
		Trojan[Banker]/Win32.Tuhkit	此威胁是一种可以窃取用户银行信息的木马家族。该家族样本运行后会连接远程服务器，收集用户系统中网络银行信息并回传。（威胁等级中）
		Trojan[Downloader]/HTA.Locky	此威胁是一种可以下载勒索软件的木马家族。该家族样本是 Html Application 应用程序，运行后会连接远程服务器下载 Locky 勒索软件并执行，会加密用户重要数据。（威胁等级中）

微软修复谷歌公布的漏洞

Michael Mimoso / 文　安天公益翻译小组 / 译

近日，谷歌研究人员披露了一个用于公开攻击的零日漏洞。随后，微软展开调查并随后修复了漏洞。谷歌在 10 月 31 日披露了该漏洞，在此 10 天前，已私下向微软报告了该漏洞，并向 Adobe 公司报告了一个 Flash 零日漏洞。

Adobe 公司在 10 月 26 日发布紧急更新，修复了 Flash 漏洞。但微软未公开承认该漏洞，直到谷歌公开披露。谷歌的内部政策允许供应商在 7 天内公布或修复正在被利用的漏洞。

谷歌表示，该漏洞是 Windows 内核中的一个本地提权漏洞，会导致沙箱逃脱。攻击者组合使用该漏洞和上述 Flash 漏洞，进入目标计算机。沙箱逃脱允许攻击者在内核模式下运行代码。微软在其公告 MS16-135 中说：“微软在 Win32k 内核组件的 Windows10 周年更新版本中实现了新的漏洞利用减灾措施。这些 Windows10 周年更新减灾措施基于主动的内部研究开发，终止了所有发现的案例。”

MS16-135 还修复了 Windows 内核中的两个其他提权漏洞 (CVE-2016-7215 和 CVE-2016-7246)，内核中的一个能够绕过内核 ASLR 的信息泄露漏洞 (CVE-2016-7214)，以及 Windows Browser.sys 内核模式驱动程序中的一个信息泄露漏洞 (CVE-2016-7218)。

微软近期发布了 14 个公告，其中的 6 个被评定为“关键”。MS16-132 涵盖了另一个 Windows 图形组件中的漏洞。微软表示远程代码执行打开类型字体漏洞已在 Windows 字体库中修复。该公告还修复了 Windows Animation Manager 和 Windows Media Foundation 中的远程代码执行内存损坏漏洞。

微软还为其浏览器 Edge 和 Internet Explorer 提供了累积更新。Edge 更新 MS16-129 修复了 17 个漏洞，其中大多数会导致远程代码执行。微软指出，其中两个漏洞 CVE-2016-7209 和 CVE-2016-7199 已被公布，但没有用于攻击。Internet Explorer 更新 MS16-142 修复了一个公布的漏洞，共修复了 7 个漏洞。

MS16-130 修复了 3 个关键的 Windows 漏洞：一个远程代码执行漏洞 (影响 Windows 图像文件加载处理格式错误的图像文件)，以及 Windows IME 和 Windows 任务计划程序中的两个提权漏洞。

MS16-131 修复了微软视频控件组件中的另一个远程代码执行漏洞。另一个关键公告是 IE 和 Edge 的 Adobe Flash Player 更新，Adobe 今天发布了一个 Flash Player 更新，修复了软件中的 9 个远程代码执行漏洞。

一个 Office 公告 MS16-133 被评定为“重要”，但也值得注意，因为它修复了 12 个漏洞，包括导致远程代码执行的 10 个漏洞。微软说，这些 Office 漏洞都没有被利用。

微软在 MS16-136 中修复了 SQL Server，解决了 6 个提权和信息泄露漏洞。3 个提权漏洞在 SQL Server RDBMS 引擎中，一个跨站点脚本漏洞在 SQL Server MDS 中，一个信息泄露漏洞在 SQL 分析服务中，另一个提权漏洞在 SQL Server 引擎服务器代理中。

Tripwire 的安全研究员 Craig Young 说“：大多数管理员的首要任务是快速部署浏览器、图形组件和 Office 的修复程序。所有这些组件都受到微软评定为“高度可利用的”的一个或多个代码执行漏洞的影响。由于这些漏洞能够通过正常的网络浏览活动触发，使外部攻击者进入网络，因此它们是最高优先级的。”

以下公告也被评定为“重要”：

- MS16-134 修复了修补程序在 Windows 通用日志文件系统 (CLFS) 中的 10 个提权漏洞。
- MS16-137 修复了 Windows NTLM，虚拟安全模式和本地安全机构子系统服务中的 3 个漏洞。
- MS16-138 修复了 Windows 虚拟硬盘驱动程序中的 4 个提权漏洞。
- MS16-139 修复了 Windows Kernel API 如何实施权限的本地 Windows 内核提权漏洞。
- MS16-140 修复了 Windows 安全启动组件中的安全功能绕过漏洞，攻击者可以由此禁用代码完整性检查，并允许加载测试签名的可执行文件和驱动程序。

原文名称	Microsoft Patches Zero Day Disclosed by Google
作者简介	Michael Mimoso，卡巴斯基《安全周报》编辑。
原文信息	2016 年 11 月 8 日发布于《安全周报》(Threatpost)，原文地址 https://www.linkedin.com/in/michaelmimoso
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《Rex 木马样本变种分析报告》

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 Rex 的木马进行了简要分析。

最初人们认为 Rex 木马是一个勒索软件，利用易受攻击的 Drupal 网站加密他们的文件，并索要赎金。而后续的分析表明，Rex 木马在对设备进行初始感染之后还具有其他恶意行为，例如启动 DDoS 攻击、锁定网站、挖掘加密货币等。

经分析，Rex 木马样本更多地作为渗透工具，而不是 DDoS 攻击。攻击者会利用 Drupal，WordPress 和 Magento 网站中的漏洞，来感染 Linux 设备，以及 Exagrid，Apache Jetspeed 和 AirOS 家庭路由器等应用程序。当被攻击目标受到感染后，攻击者会向网站管理员发送电子邮件，进行索要比特币，以此来威胁发动 DDoS 攻击。

针对 Drupal，Rex 木马会利用 CVE-2014-3704 漏洞进行感染。此漏洞是一个 SQL 注入漏洞，允许木马病毒创建一个管理帐户，因此攻击者通过它可以控制 CMS。针对 WordPress，Rex 木马样本既不锁定网站也不显示赎金提示，而是运行其他的恶意功能，试图利用 WordPress 网站中如 WooCommerce，Robo Gallery，Rev Slider，WP-squirrel，Site Import，Brandfolder，Issuu Panel 和 Gwolle Guestbook 等插件中的一些安全漏洞。针对 Magento，Rex 木马样本会通过 Shoplift RCE 漏洞 (CVE-2015-1397，CVE-2015-1398 和 CVE-2015-1399) 进行定位创建一个管理员帐户并控制底层 Web 服务器。

Rex 木马还在继续演变，其样本的作者采用了最近泄露的 Mirai 源代码，并将其一些组件添加到 Rex 木马中。最初，他们移植了用于扫描易受攻击设备的 Mirai 组件并威胁设备的 Telnet 端口。不过这个实验没有成功，研究人员跟踪了 Rex 样本的演变，发现包括 Mirai Telnet 扫描仪的 Rex 样本变体感染力并不强，只能感染大约 10 个设备。由于 Rex 移植 Mirai 功能失败，所以 Rex 的作者只能从更成熟的 IoT/Linux 恶意软件去移植。目前，Rex P2P 僵尸网络大约可以控制 150 台机器，用于对企业进行 DDoS 攻击。

通过对 Rex 木马样本的分析了解，可以看出恶意代码感染手段的多样性，恶意目的各不相同，为了避免企业与个人的损失。安天提醒用户要提高网络安全意识，日常工作使用电脑要养成良好习惯，经常杀毒，不随意查看异常邮件，发现网络异常要提高警惕并及时采取应对措施。目前，安天追影产品已经实现了对 Rex 恶意样本的检出。

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、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。

最终依据智能学习鉴定器将文件判定为木马程序。

该文件具有以下行为：创建进程、读取文件、随机绑定本地端口、UDP 访问本机端口。

文件名	0653353E659B2AB5D761B5839729B3C4
文件类型	BinExecute/Linux.ELF
大小	1.94 MB
MD5	0653353E659B2AB5D761B5839729B3C4
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Linux.Rex
判定依据	智能学习

◆ 运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
创建进程	★★★★	读取文件	★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
随机绑定本地端口	★	UDP 访问本机端口	★

◆ 运行环境

描述	值	描述	值
File Size	1990 kB	File Type	ELF executable
MIME Type	application/octet-stream	CPU Architecture	32 bit
CPU Byte Order	Little endian	Object File Type	Executable file
CPU Type	i386		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=0653353E659B2AB5D761B5839729B3C4