安天周观察

安天官方微博　安天官方微信

主办：安天　2017 年 12 月 18 日 (总第 116 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

【红旗漫卷】第五届安天网络安全冬训营即将启幕！

安天网络安全冬训营始于 2014 年，至今已成功举办四届，继“凛冬将至”、“北风乍起”、“朔雪飞扬”、“冰峰屹立”之后，**第五届安天网络安全冬训营——“红旗漫卷”将于 2018 年 1 月 11、12 两日在哈尔滨举行。**

历经五年的沉淀积累，安天网络安全冬训营（以下简称“冬训营”）现已成为直面威胁场景，业界专家交流沟通产业方向、行业趋势及产业合作的重要渠道，同时也为安全从业者及爱好者搭建了学习交流的良好平台。本届冬训营将邀请多位重量级嘉宾与安天一起进行多方威胁分析、研究进展解读及实践经验分享，为应对新时代的网安之战，提供新的防御思路。

红旗漫卷，勇担重任

在十九大报告中，总书记要求我们**“坚持总体国家安全观”、“加强国家安全能力建设”、“更加自觉地维护我国主权、安全、发展利益”**，为我国网络空间安全发展指明了方向，**“注重军民融合”、“建设网络强国”**更是给网络安全创新提供了大空间、大舞台。面对武装到牙齿的对手，打破旧有的以“物理隔离 + 好人假定 + 规定推演”构成的自我麻痹，让安全解决方案和产品具有真实有效的安全价值，迫在眉睫。为此，本届冬训营将以**“敌情想定是前提，网络安全实战化”**为主题，聚焦有效的敌情想定，面向真实的安全威胁，以期通过实战化的网络安全防护要求，为用户实现有效的安全价值。

网络空间是至关重要的非传统安全领域，网络安全能力既是非传统安全领域的关键能力，也是对政治、军事、经济等传统安全领域的强大支撑。回顾安天的十七年历程，作为习总书记肯定的“民企国家队”，安天深刻理解自身的价值使命。每一起严重威胁，安天都第一时间启动分析响应；每一次重大安保，安天都积极主动担当责任，为国家的高速发展保驾护航。

实践分享，亮剑安全

中国正在从网信领域的弱者，逐渐变成强者；从信息化技术的单纯引进者，变成部分技术的输出者。如何响应总书记网络强国的号召和网络对科技创新的要求，如何进一步深化我们的核心技术能力，将自身安全防护技术转化为真实的防御感知能力，是安天长期探索的问题。

2017 年是安天“第三次创业”的关键一年，在这场更好对接国家网络安全使命、全面进军政企安全市场的新征程中，安天围绕和能力型安全友商共同确立的“滑动标尺”基础安全模型，渐进提升安全规划能力，分析自身长项和短板。安天进一步加速“下一代威胁检测引擎”、“全要素采集”等核心技术能力开发，将传统检测器改造为检测解析器，为感知分析形成可靠大数据基础，发挥载荷检测的传统优势，同时进一步增强信标、场景和操作行为的检测与画像能力。安天探海、追影、智甲等产品不断进行能力迭代，基于态势感知、网络靶场演练等解决方案取得了更多客户认可。安天立足自身分析、研判团队的专家经验，推出了“高阶威胁情报”服务。

安天继续发挥在国家应急支撑体系中的重要作用，“魔窟”（WannaCry）勒索软件爆发后，安天在第一时间启动 A 级信息安全灾难响应，迅速发布了分析报告、防护手册和专杀工具。发布了《NSA 系列外泄网络军火级漏洞应对手册》，全面梳理了相关风险，提供了方案建议。针对乌克兰遭到的“勒索”攻击，安天第一时间上报，并提出本次事件可能不是以勒索为目的而是以瘫痪基础设施为目的的猜测，被后来的分析证实。

在本届冬训营中，我们将对在端点防护、流量监测、深度分析、态势感知等方面的最新研究进展进行介绍，分享实践成果、实战价值与未来规划。

本届冬训营官网（wtc.antiy.cn）现已正式上线，诚邀各位网络安全行业的专家学者、从业者及爱好者参会！安天将以更加积极主动的姿态，直面威胁，勇敢担当。雪峰险峻，红旗漫卷，长缨在手，勇缚苍龙！

每周安全事件

类 型	内 容
中文标题	12 月微软补丁解决了 19 个关键的浏览器问题
英文标题	December Microsoft Patch Tuesday addresses 19 Critical browser issues
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	微软发布了针对 2017 年 12 月的补丁更新，解决了 30 多个漏洞，其中包括 19 个影响 Internet Explorer 和 Edge 网页浏览器的严重漏洞。 微软解决了一些可以被利用来进行远程代码执行的内存损坏漏洞。大多数漏洞都存在于浏览器的脚本引擎中，攻击者可以通过欺骗受害者访问特制网站或恶意广告网站来触发他们。 本月确定的漏洞列表包括 CVE-2017-11927 追踪的“重要”信息泄露漏洞。该漏洞影响 Windows：//protocol handler，其中 InfoTech 存储格式（ITS）是 CHM 文件中使用的存储格式。 Microsoft 解决的漏洞列表还包括 Office 中的一系列信息泄露问题，影响 SharePoint 的特权升级漏洞，Exchange 中的欺骗性问题以及 Excel 中的远程代码执行漏洞。
链接地址	http://securityaffairs.co/wordpress/66676/security/december-microsoft-patch-tuesday.html

每周值得关注的恶意代码信息

经安天【CERT】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

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.Sdljfkh.a[prv,spy] 2017-12-11	该应用程序为银行木马，监听收件箱短信上传，访问银行钓鱼网址，诱导用户输入账号密码，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.SocketSpy.a[prv,rmt,spy] 2017-12-12	该应用程序运行会与服务端建立连接，通过远程指令执行窃取用户短信、私自打电话、拦截短信、发送短信、添加联系人等危险行为，造成用户隐私泄露，建议卸载。（威胁等级中）
		G-Ware/Android.daishua.a[rog,pay,exp] 2017-12-12	该应用程序为虚假代刷类应用，欺诈诱导用户付费使用，可能造成用户资费损失，建议卸载。（威胁等级高）
		G-Ware/Android.6hoAds.a[exp,rog] 2017-12-14	该应用程序运行后隐藏图标，强制要求用户给予设备管理器权限以防被卸载，否则锁屏，包含恶意代码，私自通过 http 加载广告。造成用户流量消耗，影响手机正常使用，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.FakeSystem.z[exp,rog]	该应用程序伪装成系统应用，安装无图标，运行请求激活设备管理器，加载子包，后台推送广告，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.Hqwar.j[prv,exp,rog]	该应用程序运行会请求激活设备管理器，隐藏图标，判断是否模拟器运行，监听短信联网上传短信信息，获取远程指令，执行拦截短信和发送短信的行为，造成用户隐私泄露和资费消耗。（威胁等级高）
		Trojan/Android.Dendroid.i[prv,rmt,spy]	该应用程序伪装正常应用，运行后隐藏图标，激活设备管理器权限，后台接收远程控制命令，窃取用户短信、联系人、通话记录、浏览器历史记录、地理位置等隐私信息，私自下载提权文件，删除用户短信，私自进行录音、录像、拍照，私自锁屏，解锁。造成用户隐私泄露，损害手机安全。请立即删除。（威胁等级中）
		G-Ware/Android.RogAd.z[rog,exp]	该应用程序运行弹出推广页面，需要下载推广应用才能正常使用，还会加载子包后台推送广告，造成用户资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.BankerSpy.d[prv,spy]	该应用程序伪装安全防护，运行后拦截用户短信，上传用户短信箱、联系人、手机基本信息、银行相关隐私信息。造成用户隐私泄露，建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Malware Protection Engine 远程代码执行漏洞（CVE-2017-11937）	微软官方发布了一则通告表示其恶意软件防护引擎（Malware Protection Engine）存在一个远程代码执行漏洞（CVE-2017-11937）。该漏洞源于防护引擎没有正确扫描特制的文件，导致内存损坏。成功利用此漏洞的攻击者可以在 LocalSystem 账户的安全环境中执行任意代码并控制系统。随后攻击者可以安装程序，查看、更改或删除数据；或者创建具有完整用户权限的新账户。（威胁等级高）
	较为活跃样本	Trojan[Dropper]/Win32.Daws	此威胁来自一种具有捆绑行为的木马类程序。该家族木马感染用户系统后，会自动释放出其它恶意程序并运行。释放的程序大多为盗号类木马程序。（威胁等级中）
		Trojan[Downloader]/Win32.BaoFa	此威胁来自一种具有下载行为的木马类程序。该家族可以通过共享软件或游戏捆绑安装，也可以通过邮件或恶意网站传播。家族运行后会写入注册表实现自启动，还会留下后门供黑客入侵电脑。（威胁等级中）
		Trojan[Downloader]/Win32.Adnur	此威胁来自一种具有下载行为的木马类程序。Adnur 家族木马感染用户系统之后，会修改系统设置，下载并执行多种恶意软件。（威胁等级中）

避免身份盗用的十个方法

Toni Birdsong / 文　安天技术公益翻译组 / 译

在如今的数字世界中，各大公司存储着我们的很多个人信息，因此没有人能够 100% 防止欺诈。当 Equifax 遭到黑客攻击时，很多人如梦初醒。在受 Equifax 事件影响的 1.45 亿人中，大多数都必须在未来几年密切关注他们的信贷活动。

不过，我们可以采取一些措施来减少身份盗用或网络欺诈的可能性。要注意：任何拥有社保号的人都可能成为身份盗用的受害者——包括您的孩子。以下措施也适用于孩子的身份信息保护。

1. **勇敢说“不”！**在社交平台、电子邮件注册、民意调查、调查问卷和应用程序上提供个人信息之前，需要进行辨别。网站要求你提供个人信息并不意味着有必要提供，我们应询问是谁需要这些信息和原因。不要点击诱饵链接：如果有人发给你“有趣”的社交媒体应用和游戏链接，鼓动你打开看看你跟哪个名人长得像，请无视他们！这些诱饵旨在收集你的个人信息，它们缺乏安全保障，不值得冒险。不要在社交网站上，甚至在帖子中发布你的出生日期、母亲的娘家姓、宠物的名字，或其他个人信息——许多人在网上发布信息时使用孩子名字的首字母缩写。锲而不舍的盗贼可以使用东拼西凑得来的信息验证您的身份并访问您的电子账户。

2. **放慢速度。**这个信息世界宠坏了我们，我们希望随时获得我们想要的信息。骗子们吃准了我们步履匆匆，很可能不会花时间质疑一个可疑的链接。所以在点击链接之前，请务必三思。这同样适用于我们的网络搜索，在一个可以用谷歌搜索所有东西的网络世界中，安全是至关重要的。诸如 McAfee WebAdvisor 这样

的工具可以识别恶意网站，并在用户点击之前提醒用户，从而保护用户安全。另外，搜索引擎虹吸个人和行为数据。因此，作为额外的保护层，请进入您的浏览器并修改隐私设置，以阻止广告商的追踪。

3. **粉碎纸质信息。**之前我以为这种做法太过老派，但是安全专家也赞同这种方法：如果您没有碎纸机，那么您应该考虑买一个了。纸质邮件导致的身份盗窃仍然是一个问题。您应该粉碎任何包含下述信息的纸质资料：

- 您的社保号(甚至只是最后四位数)
- 您的出生日期
- 您的信用卡号
- 来自金融机构的任何账号
- 医疗保险号
- 不请自来的信贷申请

4. **莫忘基本的安全措施。**不管你认为自己对技术和风险了解多少，都要保持一颗谦逊的心。您应该关注基本的隐私保护措施，包括更新密码、在社交网络上修改隐私设置、不使用公共 Wi-Fi、使用两步身份验证进行登录等。

5. **更新杀毒软件。**定期更新病毒防护软件，不要从陌生人那里下载文件。而且，当您收到更新软件的警报时——无论是手机、笔记本电脑还是平板电脑——都要注意。及时更新软件能够为安全加一把锁，否则，犯罪分子可以利用旧版本中的漏洞侵入您的设备。

6. **保护您的家庭网络。**当涉及到家庭网络时，请限制您的信任圈子——这样做可以从物理上和经济上保护您的整个家庭。请不要用姓氏命名家庭网络，也不要随意将家庭网络的密码告知他人，要像保护房子钥匙一样保护网络密码。您可以考虑创建访客网络，以便访客能够在不访问您家庭的其他连网设备或共享文件的情况下连网。

7. **了解迹象。**如果窃贼正在使用您的数据，您可能会发现以下迹象：1）通过邮递形式到达的预先批准的信用卡；2）收款机构打来电话；3）关于拖欠账单的法院通知。如果您怀疑某人正在使用您的个人信息开立账户、申报税款或进行购买，请访问 IdentityTheft.gov。

8. **了解范围。**身份盗用不仅仅在于金钱，有时候是关于服务的。医疗身份盗用是指有人使用您的信息来获得医疗护理或福利。骗子甚至用别人的身份申请公寓租金、抵押贷款、工作和退税。

9. **冻结您的账户。**如果您认为出现了数据泄露，请要求每个信用评估机构（Equifax，Experian 和 TransUnion）冻结您的信用报告，这样能够防止其他人使用您的个人信息开设新的信用额度。您可以设置提醒，如果有人企图使用您的名字或信用，您会收到提醒。

10. **从容应对。**审查数字活动的安全性并进行一些更改花不了太多时间。只要做了所有该做的努力，您就可以从容地享受您的数字生活了，不必担惊受怕。为什么要让骗子得逞呢？在全国身份盗窃宣传月（12 月），请尽您所能对抗网络犯罪分子。

原文名称	10 Pro-Active Ways to Dodge the Traps of Identity Thieves
作者简介	Toni Birdsong。Toni Birdsong 是迈克菲的家庭安全专家。
原文信息	2017 年 12 月 1 日发布于迈克菲实验室 原文地址 https://securingtomorrow.mcafee.com/consumer/family-safety/10-pro-active-ways-to-dodge-the-traps-of-identity-thieves/
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《银行木马 EMOTET 变种分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时注意并拦截到了银行木马 EMOTET 的新变种，该木马下载器通过电子邮件传播，然后诱使受害者下载 Word 文档、打开后加载恶意宏执行 PowerShell 下载其他恶意负载，包括勒索软件、Dridex，Trickbot，Pinkslipbot 和其他银行木马。该木马在 2014 年首次出现，具有窃密和网络嗅探的功能。而此次 EMOTET 新变种的回归主要有两个原因，一个是攻击者选择针对新的目标，攻击的范围不限于银行也包括其他行业；另一个是 EMOTET 传播方式主要依赖于垃圾邮件僵尸网络传播。

首先 EMOTET 伪装成一个发票或者账单的邮件，在邮件中含有一个恶意的 URL，受害者点击恶意链接后将下载一个含有恶意宏的文档文件，受害者打开文档后将执行 Powershell 下载恶意载荷。EMOTET 到目标系统后，通过添加注册表键值建立系统持久机制，保证每次系统重启都可以自动运行。EMOTET 会收集操作系统和进程列表等信息，然后将连接到命令与控制（C & C）服务器以更新到其最新版本，并由攻击者决定发送有效载荷的类型，包括 Dridex 银行木马、僵尸网络等。除此之外，还包括一些恶意模块组件，像是垃圾邮件传播模块、网络蠕虫模块、邮件密码查看器、浏览器密码查看器。从 EMOTET 的新变种来看，已经成为一个传播其他恶意载荷的木马加载器。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。目前，安天追影产品已经实现了对该类勒索软件样本的检出。

木马程序

安天【追影威胁分析系统】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：

文件由页面手工提交，经由 YARA 自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、数字证书鉴定器、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。

最终依据静态行为鉴定器、动态行为鉴定器、智能学习鉴定器将文件判定为木马程序。

根据页面手工提交得出该文件具有以下行为：其他进程写入可疑数据、删除自身、延时、查找指定内核模块、创建挂起的进程、访问其他进程内存、查找特定窗体、创建特定窗体、获取驱动器类型、获取计算机名称、请求加载驱动的权限、打开自身进程文件、释放 PE 文件、复制自身文件、获取系统版本、设置自启动项、遍历进程、获取主机用户名称、查找浏览器进程、独占打开文件获取系统内存、获取 socket 本地名称、连接网络等行为。

文件名	EMOTET-a0f765e544ac085b80fe9652fff67f95db02b4b6b07d6b78de33897986292471
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	252 KB
MD5	AE5211B90C6A2A341E2CE25B23D5A9EA
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Banker]/Win32.NeutrinoPOS
判定依据	静态分析

◆ 运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 危险行为

行为描述	危险等级	行为描述	危险等级	行为描述	危险等级
其他进程写入可疑数据	★★★	删除自身	★★★★	延时	★★★

◆ 常见行为

行为描述	危险等级
查找指定内核模块	★
创建挂起的进程	★★
访问其他进程内存	★
查找特定窗体	★
创建特定窗体	★
获取驱动器类型	★
获取计算机名称	★
请求加载驱动的权限	★
打开自身进程文件	★
……	……

◆ 进程监控

PID		命令行
1600	C:\6be7e1f2aecc40a5af2c366c39f1b8b1\share\target.exe	"C:\6be7e1f2aecc40a5af2c366c39f1b8b1\share\target.exe"
……	……	……