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 25 日 (总第 117 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

第五届安天网络安全冬训营主题解读

本届冬训营以“敌情想定是前提，网络安全实战化”为主题，旨在打破旧有以“物理隔离 + 好人假定 + 规定推演”构成的自我麻痹式的安全观，以真实的敌情想定为前提，以实战化作为网络空间安全防护的第一要求，向承担着关键信息基础设施防御使命的政企单位输出能用得起来的安全能力，帮助客户全面落实网络安全防御职责，使安全防御体系能够随时应对真实的威胁，实现有效的安全价值。

网络空间战场上的隐匿的对抗较量持续不断，因此必须把“召之即来、来之能战、战之必胜”作为检验实战化网络安全防护的标准，使“用得起来”成为检验安全技术与产品能力转化的基本要求，扭转以往针对大规模紧急事件的被动应急模式，在日常工作中积极主动地发现威胁并有效对抗。网络安全实战化，可以成为推动政企单位加大网络安全投入的新目标，也能够成为网络安全产业发展壮大的驱动力。

同时，在敌情想定的基础上，实战化也意味着能力的结合。即使再复杂的高级威胁，一线的安全运维人员都可能发现蛛丝马迹，并在专业安全分析服务人员的支持下，共同处置与对抗，打赢面对威胁的战斗！

工匠精神筑安全——安天李柏松获评“哈尔滨大工匠”

12 月 21 日，2017 年“哈尔滨大工匠”颁奖仪式举行，安天副总工程师、高级工程师李柏松与另外 17 位来自各行业的优秀工作者，共同获得“哈尔滨大工匠”的荣誉称号。

“哈尔滨大工匠”推荐选树活动由哈尔滨市总工会开展，旨在深入贯彻落实党的十九大精神，弘扬劳模精神和工匠精神，营造劳动光荣的社会风尚和精益求精的敬业风气。此次选树活动经过谨慎评审与实地考察，在 96 家单位推荐的 137 名候选人中共选树出“大工匠”18 人。李柏松是本届“哈尔滨大工匠”中唯一的网信领域工作者，其长期从事安全威胁分析与应急响应工作，十七年如一日奋斗在与网络安全对抗的第一线。

安天的核心能力是工程体系能力，安天的企业文化是工程师文化，这种严谨而踏实的文化氛围孕育了一批具有“工匠精神”的工程师，李柏松便是其中之一。

李柏松是安天第一版本反病毒引擎的主要开发人员之一，负责病毒库的设计工作。此后组建了安天的病毒分析组，这正是安天安全研究与应急处理中心（安天 CERT）的前身。安天的应急能力以“第一时间启动，同时应对两线威胁，三体系联动，四作业面协同”为建设目标，安天 CERT 正是支撑安天应急能力的枢纽部门，曾被有关部门称为“应急之魂”。作为安天应急分析工作的负责人，李柏松组织同事们依托安天感知和分析体系，针对重大和新兴威胁，开展深度分析和快速响应工作。他在“口令蠕虫”、“震荡波”、“冲击波”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情的应急响应工作中，在“震网”、“毒曲”、“火焰”、“方程式”、“白象”等 APT 行动的跟踪分析和追踪溯源中，作为一线指挥员，身先士卒，冲锋在前，带领团队形成了大量有价值的技术文献资料和重量级的分析报告，为国家积累了战略博弈素材。

李柏松被评选为省、市劳动模范，2013 年他带领同志们成立了“李柏松劳模创新工作室”，形成了党员干部、劳动模范带头值守，抢先应急的工作风格，工作室在 2014 年被授予“省劳模创新工作室”、“市示范性创新工作室”、“工人先锋号”称号。2016 年 5 月 25 日，习总书记视察安天时，曾与他互动，亲切地拿起他胸前的五一劳动奖章仔细端详。

李柏松曾说过“不懂网络安全的人是幸福的人，我们的责任是保卫他们的幸福”，这句话成为很多业内同仁的签名档，并写入了安天团队宣言。这份责任感及背后所为之付出的努力和坚持也是安天的集体追求。安天亦将不忘创业的初心，以保障国家网络安全为己任，以做好网络安全“国家队”的坚毅信念匹配习总书记的要求和嘱托，以自身在威胁检测防御核心技术积累和形成的感知分析优势能力，以“工匠精神”打造新时代的网络安全产品和服务，为捍卫国家主权、安全和发展利益，为保障用户安全价值作出更多贡献。

安天李柏松（左数第三位）获“哈尔滨大工匠”称号

每周安全事件

类 型	内 容
中文标题	BlackEnergy，DragonFly 和 TeamSpy 攻击之间的细线
英文标题	The thin line between BlackEnergy, DragonFly and TeamSpy attacks
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	赛门铁克今年 9 月发布了关于“DragonFly 2.0 行动”——针对数十家能源公司进行黑客攻击的详细分析报告，研究团队发现这些攻击活动在技术、战术和程序方面都存在相似之处，他们怀疑 “DragonFly 2.0 行动”与 2014 年观察到的 DragonFly 攻击行动背后是同一个黑客组织。 研究人员通过对恶意软件的关联分析，发现前两款恶意软件都使用了 TeamSpy 恶意软件中相同的 TeamViewer（由匈牙利安全公司 Crysys 分析提出）。 尽管此前的分析报告倾向于将黑客攻击归因于一个或多个黑客组织、认为他们彼此分享了攻击战术和工具，但研究人员同时表示，黑客组织 TeamSpy 背后的动机与 DragonFly 类似。 在通过对比 2015 年 10 月 31 日在乌克兰被捕获的 BlackEnergy 样本代码与 DragonFly 样本后，研究人员发现他们之间的这段代码几乎都是相同的，因此揭示了 BlackEnergy 和 Dragonfly 之间的相关性。
链接地址	http://securityaffairs.co/wordpress/66867/apt/blackenergy-dragonfly-teamspy-attacks.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.8uu8.a[prv,spy] 2017-12-18	该应用程序伪装正常应用，运行后窃取用户的多媒体数据、短信、手机基本信息，拦截指定短信，私自发送短信、录音并上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.UrlSmsSend.a[exp,sms] 2017-12-18	该应用程序运行后隐藏图标，访问指定网页，群发、拦截、删除短信，上传手机固件信息，可能会造成资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.TelegramIR.a[prv,rmt,spy] 2017-12-20	该应用程序是一款针对伊朗地区的间谍软件，使用 Telegram Bot API 通讯，实现远程监控用户短信、通话记录，获取固件信息、通话录音、图片、账户信息、地理位置信息，还可以远控摄像头拍照，修改用户本地文件。会造成用户隐私泄露，建议卸载。（威胁等级高）
		G-Ware/Android.ymkj.a[exp,rog] 2017-12-21	该应用程序伪装成系统应用，安装无图标，运行后释放广告子包，后台推送广告，造成用户资源损耗，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.MyVk.d[prv]	该应用程序伪装正常应用，包含恶意代码，运行后加载恶意脚本，窃取用户 VK.com 的凭据信息，并上传至服务器。造成用户隐私泄露，建议卸载。（威胁等级高）
		G-Ware/Android.WhereareMe.a[rmt,prv,exp]	该应用程序安装无图标，监听、拦截短信，还会根据短信指令响铃、振动、私自发送短信、获取用户通话信息、获取地理位置信息等。会造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.CPUMiner.d[exp,rog]	该应用程序伪装系统应用，运行隐藏图标，后台私自挖矿，会占用设备内存，同时造成损耗，建议卸载。（威胁等级中）
		Trojan/Android.Mobilespy.at[prv,rmt,spy]	该应用程序伪装系统应用，运行隐藏图标，接收远程指令上传用户手机固件、电话号码、Gmali 邮箱账号等隐私信息，还会通过远程数据动态加载未知子包，警惕其窃取短信、联系人、通话记录等隐私信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		G-Ware/Android.Clicker.m[exp,rog]	该应用程序伪装正常应用，运行隐藏图标，诱导激活设备管理器，私自访问指定链接，警惕该程序私自下载或诱导点击推广内容，造成用户资费损耗，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	Linux 内核的 Huge Dirty COW 权限提升漏洞（CVE-2017 - 1000405）	当新页面可写时会将原始“只读”页面复制到新页面，而原始页面可能是具有“特权”的，由此造成了 Linux 内核的 Huge Dirty COW 权限提升漏洞。（威胁等级高）
	较为活跃样本	Trojan[Backdoor]/Win32.Floder	此威胁来自一种可以窃取用户信息的木马家族。它会自动将原文件及其根目录下文件夹隐藏，同时将文件后缀名隐藏，生成与文件夹同名的应用程序文件，并设置为文件夹图标，大小为 44K，使用户误认为是自己的文件夹；运行后连接远程服务器，可以窃取用户信息并回传。（威胁等级高）
		Trojan[Ransom]/Win32.CryptoBit	此威胁来自一种勒索者家族程序。这家族的样本伪造播放器图标，对文档加密，连接 C&C 服务器（laoismacau.com/58.64.142.89，未使用 DGA），并在多个文件夹下留下勒索信 "HITLER HAS YOUR FILES"，在「我的文档」留下被加密过的文件的列表。CPU 占用较低，不易察觉。（威胁等级中）
		Trojan[Ransom]/Win32.Zerber	此威胁来自一类可以加密用户数据的木马家族。该家族样本是勒索软件，运行后加密用户文件，加密后播放声音提示用户文件已被加密，需支付比特币才可以解密。（威胁等级中）

机器学习的十个出人意料的用途

Roxanna "Evan" Ramzipoor / 文　安天技术公益翻译组 / 译

随着机器学习技术的发展，各个领域的开发人员开始寻找解决难题的创新方法。

机器学习（ML）正在风靡科技世界。事实上，ML 技术的一些最近的应用不仅具有创新性，而且有些怪异，令人惊讶。其他领域的公司和研究人员也开始以一种令人惊讶的方式使用 ML 技术。以下是机器学习的十个出人意料的用途。

预测刑事被告是否具有潜逃风险（flight risk）。法官经常需要决定刑事被告在监狱还是在家里等待审判。这是一个棘手的问题。一个由经济学家和计算机科学家组成的团队利用数十万纽约市案件的数据，训练了一种算法，以预测被告是否具有潜逃风险。该算法借鉴被告的逮捕记录来制定决策。当对以前从未见过的案例制定决策时，该算法的表现胜过有经验的法官。

利用推文来诊断精神病。研究人员现在有数据表明，某些推文模式和精神病之间存在关联。他们借鉴 2011 年的一项研究确定被诊断的精神病患者的语言模式，以建立一个机器学习算法，在推文中找到这样的模式。参与者完成一项旨在衡量诸如马基雅维利主义、自恋、开放性和外向等性格特征的自我评估。之后，ML 系统分析，经常咒骂，喜欢使用“我们”（we）、“憎恨”（hate）、“我是说”（I mean）和“呃”（um）等填充词的 Twitter 用户更有可能患精神病。

帮助选手赢得环法自行车赛。大约有 200 名选手参加比赛环法自行车赛，电视台工作人员不会一刻不停地拍摄所有参赛者，因此比赛开始后教练和参赛者很难确定自己的策略。WinningAlgorithms 是一个机器学习系统，可以沿着环法自行车赛的路线挖掘观众的社交媒体信息，因为观众可以提供他们最喜欢的自行车选手的最新数据。该算法还具有从虚假信息中筛选事实的能力。

识别濒临灭绝的鲸鱼。康奈尔大学的生物声学研究计划正在使用机器学习技术来减少航运船舶的环境影响。为了保护最后的 400 头鲸鱼，康奈尔大学的研究人员使用录制的鲸鱼叫声数据集来训练机器学习系统。然后，他们部署了一个全球浮标网络，用于扫描海洋中的鲸鱼叫声，根据叫声距离预测鲸鱼的位置和航迹。

翻译法律术语。法律文件不容易理解。但并不是每个人都有时间或资源去聘请一名律师，Legal Robot 创建了一个将法律语言翻译成日常语言的机器学习模型。通过深度学习和地理数据分析，Legal Robot 既可以处理法律术语，也可以确定合同中是否包含不应存在的条款，例如保密协议中的专利使用费。

防止洗钱。在检测到一个看起来像洗钱的异常交易后，分析师会遵循一个标准的程序：他们设计一个“好的解释”和一个“坏的解释”。但是，与任何手动系统一样，这个程序是不完善的。这就是为什么 PayPal 设计了一个机器学习系统来防止洗钱。通过使用深度学习和其他工具，该系统可以比人类分析师更准确地判断合法与非法交易。

确定留言板上的哪些主题将被关闭。像任何在线论坛一样，Stack Overflow 的很多帖子都没有价值，具有煽动性，或者离题万里。考虑到版主每天看到大量的帖子，他们有时候很难从中筛选出好的帖子。为此，Stack Overflow 举办了一个比赛，要求用户创建一个机器学习程序，以预测某个主题何时关闭。获胜的用户创建了一个以惊人的准确度预测主题关闭时间的模型。

预测医院等待时间。任何在急诊候诊室待过的人都知道医院等待时间的不可预测性。一组研究人员开发了一种可以预测医院等待时间的机器学习算法。该系统权衡不同的变量——是否是假期周末、外面有多冷、多少医务人员值班等——计算病人的等待时间。随着时间的推移，该系统的准确性也会增加，因为它会更多地了解一些因素，例如星期六有多少人看病，或者某一天有多少医务人员请假。

计算拍卖价格。专家通常很容易预测历史文物、名画或稀有汽车等珍贵物品的销售价格，二手机械（如推土机）一直在拍卖，但是，每次拍卖的价格差异很大。现在根据广泛的数据（从机器轮胎尺寸到类似设备的历史拍卖价格）对机器学习模型进行训练，可以预测最终售价，准确率超过 60%。

预测地震。每年大约有一万人死于地震，因此研究人员一直在寻找预测地震和震级的方法。洛斯阿拉莫斯国家实验室（Los Alamos National Laboratory）的两位科学家在这方面迈出了关键的第一步。他们创建了一个地震模拟模型，该模型由裂缝（或者“断层线”）隔开的模块组成。然后，他们训练一个机器学习算法来检测模型的声发射。这个 ML 模型准确度惊人，甚至能够提前一段时间检测到地震——这在很大程度上避免了地质学家的困扰。

原文名称	10 Surprising Ways Machine Learning is Being Used Today
作者简介	Roxanna "Evan" Ramzipoor，Roxanna“Evan”Ramzipoor 是 Sift Science 的作家。
原文信息	2017 年 12 月 13 日发布于 InformationWeek 原文地址 https://www.informationweek.com/big-data/ai-machine-learning/10-surprising-ways-machine-learning-is-being-used-today/a/d-id/1330613?
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《窃密木马 SEVESS 样本分析报告》

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到一款新出现的后门木马 SEVESS。该木马拥有搜集用户信息上传 C2 服务器、查看修改用户注册表、创建服务、删除自身、搜索系统进程、创建互斥量等功能。病毒启动后，首先判断命令行参数中是否含有 WIN7 字样，如果有，启动工作进程；如果没有，启动安装进程。程序首先更改注册表中 windows 最新的更新时间（更新为当前时间）。复制自身到 C:\windows 目录下并随机命名，之后注册服务 Fghijk Mnopqrst Vwx。创建 VBS 脚本并启动达到删除自身的效果。启动服务后，创建互斥量 hc58.msns.cn。连接 C2 服务器（hc58.msns.cn）并启动接受线程。获取用户信息，检查系统进程。

首先样本会判断参数中是否包含 Win7 字样，如果存在则走 Win7 分支，接下来修改系统最新更新时间为当前时间，将自身复制到 C:\windows 目录下，随机以六个字母命名，然后调用 CreateServiceA 注册服务 Fghijk Mnopqrst Vwx 并启动。同时在 C:\windows 下生成 vbs 脚本，随机命名并启动达到删除自身的目的。网络方面，样本创建与 C&C 服务器域名相同的互斥量，连接 C&C 服务器并接收恶意指令，样本可以获取用户名、系统内存使用状况、硬件信息、操作系统信息等，它还有对抗杀软的功能，样本中硬编码了多个中文字符串，均为国内常用的杀毒软件名称，样本可以检索当前系统进程中是否含有指定进程。

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：删除自身、延时、疑似桌面控制、获取 CPU 信息、打开自身进程文件、释放 PE 文件、复制自身文件、创建服务、获取驱动器类型、启动服务查找指定内核模块、创建特定窗体、获取计算机名称、请求加载驱动的权限、获取主机用户名称、在根目录创建可执行脚本、获取系统内存、访问 dns 连接网络、获取 socket 本地名称、检查摄像头、查找反病毒程序、遍历进程、独占打开文件、自启动等行为。

文件名	ce0a28a558b07ad3d9fa7b1225e5aa09
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	96 KB
MD5	CE0A28A558B07AD3D9FA7B1225E5AA09
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.AGeneric
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
删除自身	★★★★	延时	★★★

◆ 常见行为

行为描述	危险等级
打开自身进程文件	★
释放 PE 文件	★
复制自身文件	★★
创建服务	★
获取驱动器类型	★
启动服务	★
查找指定内核模块	★
创建特定窗体	★
获取计算机名称	★
.....	.....

◆ 进程监控

PID		命令行
1628	tslnu.exe	C:\WINDOWS\tslnu.exe
1692	C:\WINDOWS\System32\WScript.exe	"C:\WINDOWS\System32\WScript.exe" "C:\9912.vbs"
.....	.....	.....