# 安天周观察

主办：安天　2017 年 10 月 9 日 ( 总第 106 期 ) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流


## 助力网安人才培养
## 安天网络空间安全学院正式成立

9 月 18 日下午，安天网络空间安全学院在哈尔滨安天总部正式成立并举行揭牌仪式。黑龙江省委网信办主任李耀东在揭牌仪式上致辞，安天首席技术架构师、安天网络空间安全学院院长肖新光介绍了学院的成立背景及发展目标。来自黑龙江省委网信办、相关高校、企业的领导和负责同志共同出席了本次揭牌仪式。在中央网信领导小组第一次会议上，习近平总书记要求“加强网络空间安全人才建设，打造素质过硬、战斗力强的人才队伍”。4·19 网信工作座谈会上，习总书记又再次强调“网络空间的竞争，归根结底是人才的竞争”，网络安全人才的培养和使用需求迫在眉睫。

为贯彻习总书记的讲话精神，为发展安全、稳定、繁荣的网络空间提供合格的人才保障，在黑龙江省委网络安全与信息化领导小组办公室及各教育主管部门的帮助与指导下，经前期筹备，“安天网络空间安全学院”正式成立。

李主任表示，安天网络空间安全学院的成立，是黑龙江省网络安全企业对于国家网信人才培养战略的积极响应和创新实践，也是站在企业的实际需求来提出人才匮乏的解决方法，有利于提升黑龙江省网信人才的数量和质量，进一步推动网信工作的高效开展，提高维护网络安全的能力和水平。安天网络空间安全学院建立的核心目的是解决安天自身人才的梯队建设问题，并兼顾社会培养需求，力求通过与高校等科研院所的合作，为网络安全人才提供实训。安天学院将以爱国主义和安全工作者的职业操守为前提，以安全架构、安全开发、安全分析、安全运维工程师培养为重点，培养面向一线的合格网络安全技术人才。

## 肖新光：为中国网络安全塑造几代人

——安天网络空间安全学院正式成立揭幕式演讲全文 ( 第 3 版 )

## 安天 2018 年校园招聘启动

2017 年 9 月 27 日起，安天 2018 年校园招聘在各地陆续开展。首场招聘会于 27 日晚在哈尔滨工业大学举行，安天技术负责人现身主讲。本次宣讲会吸引了众多学子，现场气氛热烈。

安天一直坚持走能力型安全厂商道路，成立十七年来专注于自主先进威胁检测防御核心技术的研发，目前，安天的反病毒引擎已为全球近十万台网络设备和网络安全设备、超过十亿部移动终端设备提供安全防护。

安天始终直面威胁，在红色代码Ⅱ、口令蠕虫、震网、破壳、沙虫、白象、方程式、魔窟等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。曾参与十七大、十八大、历届两会、奥运会、世博会、G20 峰会等安保工作，并多次荣获重大信息活动安全保卫工作突出贡献奖。

安天坚持以“工程师文化”为主导，秉承“正直、彪悍、专业、协作”的团队风格，以工程能力为用户解决问题。

安天长期致力于自主研发创新，在全国建设有 6 个研发中心，拥有两个省级工程中心、一个博士后流动站，历史上承担过大量 863、242 等国家网络安全领域的基础研究课题，获得过多个省部级科研奖项。近期，在黑龙江省委网络安全与信息化领导小组办公室及各教育主管部门的帮助与指导下，安天成立了“安天网络空间安全学院”，对自身员工的培养和梯队建设成长提供有力保障。

安天 2018 年校招还将登陆多所高校开展宣讲活动，安天将持续招募热爱技术、有理想、有坚持的学子们加入，一同为“直面威胁、保障价值、服务客户、解决问题”而携手奋战。


## 为客户解决问题
## ——安天“工程师文化”

在一次央视对安天的采访中，记者所使用的采访设备突发状况，出现了话筒和接收器不能正常连接的问题。安天工程师林长伟检查后发现了问题所在，并现场帮助记者进行话筒维修，很快解决了问题，使采访正常进行。记者对安天工程师解决实际问题的能力表示赞赏，并感慨“安天什么问题都能解决”。

虽然这只是一个很小的案例，但却从细微之处体现了安天的“工程师文化”。安天自创立以来，一直以“工程师文化”为主导，秉承“正直、彪悍、专业、协作”的团队风格，以工程能力为用户解决问题的“工程师文化”已融入到安天人心中。

# 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | 大规模 HerbaLife 垃圾邮件活动传播 Locky 勒索软件变种 |
| 英文标题 | Massive HerbaLife spam campaign spreads a variant of Lockyransomware |
| 作者及单位 | Pierluigi Paganini; SecurityAffairs |
| 内容概述 | 近日，研究人员发现了一种新的广泛的勒索软件活动，其利用带有恶意附件的电子邮件，其中一些假装由多个营销公司发送。电子邮件是在 24 小时内发出的，从那时起，攻击者以每小时约二百万的攻击速度发出信息。研究人员已经证实，这种攻击正在使用具有单个标识符的 Locky 变体。标识符允许攻击者识别受害者，以便当受害者支付赎金时，攻击者可以向受害者发送解密器。电子邮件附件是通过销售公司发出的订单的发票。如果用户打开文件，它将启动勒索软件样本。在这次袭击中，所有受害者都得到相同的标识符，这意味着支付赎金的受害者不会得到解密。 |
| 链接地址 | http://securityaffairs.co/wordpress/63355/cyber-crime/herbalife-spam.html |

# 每周值得关注的恶意代码信息

经安天检测分析，本周 8 个移动平台和 4 个 PC 平台的恶意代码家族值得关注

| 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.DownloadTracker.a[exp,prv]2017-09-26 | 该应用程序运行后，会检测安装环境，下载安装恶意间谍程序，造成资费消耗和隐私泄露，建议立即卸载。（威胁等级高） |
| | | G-Ware/Android.FishingMaker.a[rog,exp] 2017-09-26 | 该应用为钓鱼类应用的生成、推广程序，运行诱导用户付费，恶意制作、传播钓鱼程序，且包含恶意广告子包，通过悬浮球、插屏、私自下载广告安装包并创建桌面图标等形式进行频繁的广告推送，会造成用户资费消耗，建议不要使用。（威胁等级低） |
| | | Trojan/Android.cxbox.a[exp,rog] 2017-09-28 | 该应用程序伪装成系统应用，安装无图标显示，私自下载并加载子包，后台推送广告，造成用户资费损耗和电量消耗，建议卸载。（威胁等级高） |
| | 较为活跃的样本 | Trojan/Android.Dropper.r[exp,rog] | 该应用程序伪装成系统设置，运行后加载广告子包推送广告，造成用户流量消耗。（威胁等级中） |
| | | Trojan/Android.Locker.m[rog,sys,lck] | 该应用程序伪装成其他应用，运行请求激活设备管理器，置顶并锁定界面，要求用户付费解锁，影响用户正常使用且难以自然卸载该应用，建议不要使用。（威胁等级高） |
| | | Trojan/Android.Triada.bh[exp] | 该应用程序伪装成系统应用，安装无图标显示，私自加载恶意子包，应警惕该软件私自下载造成用户资费损耗。（威胁等级中） |
| | | G-Ware/Android.Downloader.dl[exp,rog] | 该应用程序运行私自下载恶意子包，并私自恶意添加大量用于安装应用的桌面快捷方式，造成用户流量消耗，建议不要使用。（威胁等级低） |
| | | G-Ware/Android.FakeApp.ax[exp,rog] | 该应用程序伪装正常应用，无实际功能，运行下载未知文件，私自推送广告，同时包含相关支付模块，存在私自订阅的风险，建议卸载。（威胁等级中） |
| | | G-Ware/Android.StealMoneyGame.r[pay,rog] | 该应用程序为游戏应用，其付费信息不明显，以领取道具名义频繁加载弹窗，诱导用户点击付费，造成用户资费损耗，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 | Microsoft Office Memory Corruption Vulnerability - CVE-2016-7193 (MS16-121) | 当 Office 无法处理 RTF 时，可能导致 RFT 远程漏洞执行。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。（威胁等级高） |
| | 较为活跃样本 | Trojan[Downloader]/MSWord.Steamilik | 此威胁是一种具有下载行为的木马类程序。该家族通过垃圾邮件进行传播，样本为 Word 宏病毒，运行后连接网络下载其它恶意程序并运行。（威胁等级中） |
| | | Trojan[Dropper]/Win32.Pincher | 此威胁是一种具有捆绑功能的木马类程序。该家族从用户系统窃取重要数据和信息，并将其发送给攻击者。该家族将恶意代码注入到被感染系统，并防止用户访问 Windows 的注册表文件。（威胁等级中） |
| | | Trojan[Backdoor]/Win32.Dluca | 此威胁是一种可以窃取用户敏感信息的木马家族。该家族样本运行后连接远程服务器，将系统版本、屏幕尺寸、使用语言等系统信息通过 GET 请求回传给攻击者。（威胁等级高） |

# 为中国网络安全塑造几代人

■ 安天技术负责人 肖新光

**尊敬的耀东主任、尊敬的各位专家领导和媒体朋友们、亲爱的战友们：**

习近平总书记在4.19讲话中指出“建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的”。为贯彻总书记4.19讲话精神，切实推动网络安全事业持续发展，安天在黑龙江省委网信办的指导下，成立安天网络空间安全学院。安天将借助多年基础研发、安全分析的经验积累，通过广泛的高校合作及模式的创新，为安天自身、行业和国家培养输送合格的网络安全人才，保障网络空间的健康发展。

安天网络空间安全学院优先满足安天自身员工成长和规模发展需求，并进一步兼顾我国网信事业发展需要，强调以爱国主义和安全工作者的职业操守为前提，以安全架构、安全开发、安全分析、安全运维工程师的培养为重点。安天认为网络安全教育不仅仅是经验、技能教育，更要包括原则立场、科学方法和实证精神的教育。

安天长期致力于自主研发创新，在全国建设有6个研发中心，拥有两个省级工程中心、一个博士后流动站，历史上承担过大量863、242等国家网络安全领域的基础研究课题，获得过多个省部级科研奖项。安天是多所985院校的实习基地，协助高校中开设了多门课程，协助高校建设网络安全大实验，为高校提供研究资源等。安天的多位技术负责人也担任了我国多所高校的兼职教授、客座研究员、企业导师等。安天网络空间安全学院的建设不仅让安天根据自身和国家的需求打造人才梯队，也会把安天的校企合作推到一个全新高度。

当前，通过信息安全竞赛等方式，我国网络安全人才培养的热潮方兴未艾，可以说是热情高涨、形势喜人，一大批青年才俊脱颖而出，网络安全人才需求的缺口得到初步缓解，在漏洞分析、渗透测试方面的培训已经有了一些经验基础。但远程扫描、挖掘漏洞、渗透攻击只是网络安全中的一个窄带分支，CTF竞赛也不能替代有效的安全实训。我们的大量安全人才短板实际上位于规划、研发、配置、处置等方面，不能把人才中相对低端的都向脚本小子、攻击手的方向培养，把相对高端的都向漏洞挖掘的方向培养。其中还存在很多技能的不确定性和风险性。我们应避免脱离基本立场、职业底线的引导，避免脱离实际需求大比例地去培养具有“做坏事”技能的人，否则我们的信息社会将遭受到反噬。

“网络安全的本质在于对抗”，对抗是在人和人之间、组织和组织之间、国家和国家之间进行的，但它不是高手过招的模式，不是仗义行侠的模式，它的表现形式是人和人依托于综合的工程体系和能力体系进行博弈，是体系化的对抗模式。在这种体系化的对抗模式下，首先就要求有成熟可靠的产品体系、服务体系、综合规划和综合管理能力，因此这就需要大量品质纯良、遵守底线、具有成熟职业技能意识的开发工程师、分析工程师、服务工程师、配置工程师以及安全规划师。

从安天网络空间安全学院的培养导向上来看：

**第一，我们培养的是网络安全工程师。**

安天人有一个自我认知“我们不是大侠、不是明星、更不是黑客，我们是网络安全的工程师，我们以自己是工程师而自豪。工程师文化是用工程能力和方法为用户有效解决问题的文化，是安天的文化基石。

**第二，我们直面安天发展的大量人力需求和国家网络安全人才的结构短板。**

安天在发展过程中，需要大量的研发人才、分析人员，同时当前我们国家的网络安全人才培养太少考虑运行、维护、值守、处置，还有很多建设、部署、配置方面的问题，现有的整个人才课程体系中很少包含这方面的内容。从人才配比的角度来看，很多工作，尤其是运行、处置、分析工作需要大量的人力，需要人来发现问题。一个人可以发现很多问题，但每个问题又需要更多人来解决，所以从人才结构的金字塔上来看，我们需要大量能够做基本工作的同志。

**第三，我们兼顾网络安全的人才培养和信息化人员的网络安全意识和能力培养。**

信息化人才的网络安全培养、信息化用户的网络安全培养和机要办事人员的网络安全培养，必须是综合的，必须是跨体系的。

**第四，我们要立足于强调实操技能的培养体系，拿起一个系统就能做安全配置，遇到一个告警就知道该做什么。**

我们要在与威胁的对抗中、在与对手的博弈中，通过安全的实操去培养更优秀的实战工程师。

**第五，我们将培养更为复合的高级人才。**

对于中高层网络人才的培养，我们要立足网络安全，超出网络安全，越是在高层人才的培养中，对于信息化和计算机综合能力的要求就越高，对于高层人员，一定要重视跨领域和跨计算机能力的培养，改变当前网络安全人才缺少做信息系统的能力、缺少对信息系统全面认知的困境。

同时我必须强调的是，网络安全人才必须讲究政治立场。网络安全是当前大国博弈的焦点，网络安全是一个充满矛盾斗争的领域，中国的网络安全工作者肩负着为中国网络强国之路保驾护航的历史使命，必须勇敢地迎接自己的历史责任，必须站稳自己的政治立场。

美国人在二十一世纪初做出了这样的反思——“我们在信息安全领域的最大失误是在计算机发展的前20年，没有用安全的方法和视角，影响计算机的第一批使用者，而这些人将领导下一个二十年”。安天从2000年开始创业，到今天也已经17年，已经接近二十年了，我们自身出现了工程师文化退化，技术理想和追求退化的情况，我们还没有有效的整理和总结我们的方法论。现在是我们把自身的安全方法和经验总结沉淀，并将其传递给下一代安天人、传递给更多的网络安全同路人的时候。此前数年，通过将《反病毒技术》、《网络安全技术基础》的课程和实践与高校相结合，凭借安天先后在哈尔滨工业大学、武汉大学建立对口实习基地的优势，从优秀的实习生中进行选拔培养，安天培养出了以潘宣辰为代表的一批优秀青年专家。目前，潘宣辰同志已经成为了安天移动安全公司的CEO，也成长为安天最年轻的合伙人。

三年前，在安天的招聘宣讲中，我对即将加入安天的青年学子们说“让不惑的我仰望青春的你”。今天，当以小潘为代表的第二批安天人也已经到达了而立之年的时候，我们深感：理想闪耀，见目标尤远；岁月流逝，则责任弥坚。这是我们要珍惜今天的时刻，这是我们要立足长远的时刻。

我们不只保卫中国网络空间的现在，我们还要保卫中国网络空间的未来。我们是献身中国网络空间安全的一代人，我们还要为中国网络空间安全的未来塑造几代人。

**——这是安天技术负责人在安天网络空间安全学院成立仪式上的讲话**

# 安天发布《新型 Bootlocker 勒索软件 RedBoot 分析报告》

近日，安天 CERT（安全研究与应急处理中心）拦截到了新型 Bootlocker 勒索软件 RedBoot。勒索软件 Bootlocker 类型可进行对系统重要文件加密后锁定系统引导、替换系统驱动器的主引导记录和修改分区表等操作。

主引导记录（Master Boot Record，缩写：MBR），又称主引导扇区，是计算机开机后访问硬盘时所必须要读取的首个扇区。勒索软件修改 MBR 的目的是在系统重启后将显示勒索信内容。经研究分析发现 RedBoot 更像是文件擦除工具，因为该勒索软件没有提供一种方法来输入一个密钥恢复 MBR 或者分区表，除非其开发者拥有一个恢复引导的解密器。

当由微软支持的 AutoIT 脚本编译的可执行文件 RedBoot 在受害者机器中运行时，勒索软件会提取 5 个文件到系统路径中随机生成的文件夹里，其分别为 assembler.exe（该文件是编译器 nasm.exe 的重命名，用来将 boot.asm 汇编文件编译成主引导记录 boot.bin 文件）、boot.asm（用来编译成新主引导记录的汇编文件 boot.bin）、overwrite.exe（用来将系统中的 MBR 覆写为 boot.bin）、main.exe（加密系统文件的加密器）和 protect.exe（此可执行文件将终止并阻止其他程序运行，像任务管理器和进程工具等）。提取文件成功后，主启动程序将利用 assembler.exe 编译 boot.asm 文件生成 boot.bin，随即删除 boot.asm 和 assembler.exe。之后利用 overwrite.exe 将 boot.bin 覆写到当前系统的 MBR。接下来，RedBoot 启动加密系统文件流程，即执行 main.exe，扫描设备上的文件，并将“.locked”扩展名附加到每个加密文件，在此过程中通过执行 protect.exe 来防止其他进程停止加密程序。加密完成后，RedBoot 勒索软件将重启电脑，显示勒索信。

安天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。

## 勒索软件

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：

文件被页面手工提交发现，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。

最终依据动态行为鉴定器将文件判定为勒索软件。

| | |
|---|---|
| 文件名 | _RedBoot1001a8c7f33185217e6e1bdbb8dba9780d475da944684fb4bf1fc04809525887 |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 1.19 MB |
| MD5 | E0340F456F76993FC047BC715DFDAE6A |
| 病毒类型 | 勒索软件 |
| 恶意判定 / 病毒名称 | Trojan[Packed]/Win32.Krap |
| 判定依据 | 动态行为 |

### 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、GoogleChrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader |

### 危险行为

| 行为描述 | 危险等级 |
|---|---|
| 删除自身 | ★★★★ |

该文件具有以下行为：疑似桌面控制；填充导入表（疑似壳）查找指定内核模块；创建特定窗体；打开自身进程文件；获取主机用户名称；释放 PE 文件；篡改系统文件创建时间；获取驱动器类型；读取自身文件；获取计算机名称；复制自身文件。

### 常见行为

| 行为描述 | 危险等级 |
|---|---|
| 填充导入表（疑似壳） | ★★ |
| 查找指定内核模块 | ★ |
| 创建特定窗体 | ★ |
| 打开自身进程文件 | ★ |
| 获取主机用户名称 | ★ |
| 释放 PE 文件 | ★ |
| 篡改系统文件创建时间 | ★★ |
| 获取驱动器类型 | ★ |

### 进程监控

| | |
|---|---|
| PID：1880 | 创建：DesktopLayer.exe |
| | 命令行：C:\Program Files\Microsoft\DesktopLayer.exe |

完整报告地址：https://10.255.16.99/_lk/details.html?hash=E0340F456F76993FC047BC715DFDAE6A