安天周观察

主办：安天　2017 年 2 月 13 日（总第 75 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

中央政法委秘书长汪永清一行参观安天哈尔滨总部

2 月 11 日，中央政法委秘书长汪永清、科技部党组书记王志刚、中央文献研究室主任冷溶等领导莅临安天哈尔滨总部考察，观看了产品和技术演示，听取了关于安天发展状况、研发进展和产品应用等的汇报。

安天技术负责人介绍了安天威胁检测防御核心技术的工作原理、研发过程、在产业链和行业的应用情况；并介绍了安天在威胁检测引擎、安全分析与支撑体系、网络威胁监控、移动安全、工控与硬件外设安全、APT 深度分析和态势感知方面的整体技术布局，也介绍了地方政府对安天研发和发展的支持情况。

在安天应急响应中心，安天技术负责人介绍了安天持续与网络安全威胁对抗的情况，特别汇报了对高级威胁发现、捕获、分析方面所做的工作，重点介绍了安天针对“APT-TOCS”、“白象”、“方程式”等攻击组织对我方 APT 攻击情况、所使用的攻击装备等的分析进展。

在安天产品展示区，安天技术负责人为考察组领导展示了探海威胁检测系统、智甲终端防御系统、追影威胁分析系统如何在态势感知系统的协调下形成一个防御体系，并汇报了相关产品在有关部门、部委机构和行业客户的部署应用情况。

习总书记在 419 网信工作座谈会上指出，“要尽快在核心技术上取得突破，要有决心、恒心、重心，树立顽强拼搏、刻苦攻关的志气，坚定不移实施创新驱动发展战略。”在听到安天技术负责人介绍安天在 17 年的发展历程中多次经历弹尽粮绝，但坚持核心技术研发，已经在移动威胁检测等部分单点领域由最初的咬牙跟跑，实现了弯道超车时，相关负责同志表示了赞许和肯定。

安天技术负责人表示：总书记在 525 视察时对安天说“你们也是国家队，虽然你们是民营企业”，我们一定将这个要求作为看齐的标尺、努力的目标，为成为中国网络安全的国家企业而努力。汪永清秘书长表示安天人就该有这样的理想，希望安天不负期许。

国家互联网信息办公室致安天的感谢信

近日，国家互联网信息办公室向安天发来感谢信，感谢安天对国家互联网信息办公室培训中心援外培训工作的支持。

为大力宣传习近平总书记国际治网理念与主张，加强中国与发展中国家在网络安全和信息化领域的交流与合作，帮助这些国家充分了解中国互联网建设与管理的成功经验，在国家互联网信息办公室培训中心的组织下，安天讲师为古巴、哈萨克斯坦等近 20 个国家的互联网领域官员和专家学者讲解了《APT 攻击风险和案例分析》课程，受到了各方一致好评。

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的沟通和协作。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”，各类国家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。

现在，安天正积极地支持国家网络安全建设，坚持自身产业责任和基础能力建设，技术实力已得到行业管理机构的认可。安天探海等产品为很多关键客户提供了保障，多次收到来自用户、主管部门的书面感谢。

安天入选工信部 2016 年电信和互联网行业网络安全试点示范项目

近日，安天网络安全态势感知与通报预警平台最终入选了工信部 2016 年电信和互联网行业网络安全试点示范项目。这是工信部首次面向网络安全企业开展网络安全试点示范项目征集，旨在为贯彻实施网络强国战略，完善电信和互联网行业网络安全保障体系，进一步推进电信和互联网行业网络安全技术手段建设。对于入选的试点示范项目，工业和信息化部将在其申请国家专项资金、科技评奖等方面，按照有关政策予以支持。

安天网络安全态势感知与通报预警平台是一套完整的网络安全威胁监测预警与态势感知体系，具备网络攻击监测、漏洞挖掘、威胁情报收集、工业互联网安全监测等能力，实现从情报收集、威胁发现、告警、通报、感知，最终到技术处置的闭环处置流程。本平台基于高精度的网络病毒监测和捕获设备（安天探海威胁检测系统 PTD）、高级威胁鉴定系统（安天追影威胁分析系统 PTA）和安全监测处置系统（安天智甲终端防御系统 IEP），对安全威胁进行综合分析，实现及早预警、态势感知、攻击溯源和精确应对，降低系统安全风险、净化公共互联网网络环境，具体包括数据采集、安全监测、态势感知、事件告警、通报预警、追踪溯源和系统运维支撑。

每周安全事件

类 型	内 容
中文标题	新型勒索软件：只要阅读两篇有关勒索软件的文章，就可以解锁！
英文标题	Koolova Ransomware decrypts files if victims read 2 posts about Ransomware
作者及单位	SecurityAffairs；Pierluigi Paganini
内容概述	近日，安全研究专家发现了一种名为 Koolova 的勒索软件。需要注意的是，它允许用户免费恢复自己被加密的文件，这一特性与 Popcorn Time 勒索软件非常相似。但与之不同的是，Koolova 并不需要用户再去感染其他用户。 如果不幸感染了 Koolova，所要做的就是接受教育，阅读两篇关于网络安全意识的文章，学习一下勒索软件的相关知识，并且了解如何能够更好地避免感染勒索软件。学习完成之后，就可以解锁被加密的文件了。通常勒索软件会直接给用户提供一个如何支付赎金的“手把手教程”，但 Koolova 则需要被感染用户有一定的技术知识才可以找到这个页面。
链接地址	http://securityaffairs.co/wordpress/55072/malware/koolova-ransomware.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	相关描述
移动恶意代码	较为活跃的样本	RiskWare/Android.FakeApp.cz[exp]	该应用程序伪装成墨迹天气，会加载墨迹天气的网络视图，首次安装运行后，会隐藏桌面图标。影响用户体验，存在一定风险，建议谨慎使用。（威胁等级低）
		Trojan/Android.oxti.t[exp]	该应用运行后会隐藏图标，后台频繁访问色情网址，会造成用户的手机流量损耗。（威胁等级低）
		Trojan/Android.Fakesysui.k[exp，sys]	该应用安装后无图标显示，由其他应用启动，包含广告插件。运行后会尝试获取 root 权限，连网下载未知应用，并尝试静默安装。会造成用户资费消耗并面临其他威胁，建议卸载。（威胁等级高）
		Trojan/Android.Fakesysui.l[exp，sys]	该应用安装后无图标显示，由其他应用启动。运行后尝试获取 root 权限，连网下载未知应用，并提示安装，且含有 SMS 发送接收的相关代码。会造成用户资费消耗并面临其他的威胁，建议卸载。（威胁等级高）
		Trojan/Android.Erop.g[pay]	该应用会诱导用户进行点击扣费操作，点击后会私自发送扣费短信，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.FakeFlashPlayer.y[exp，rog]	该应用伪装成 Flash 应用，运行后会激活设备管理器，隐藏图标。后台窃取用户短信、联系人、应用列表等信息，并私自发送短信，会造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.Iop.i[rog，exp]	该程序包含风险代码，运行后会私自下载 APK 提权，并连网下载安装未知文件，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.QQspy.ad[prv，exp]	该应用程序会伪装成抢红包应用，程序运行后会窃取用户输入的 QQ 账号和密码等信息，造成用户隐私泄露和资费消耗。（威胁等级高）
		Trojan/Android.nbank.b[exp，prv]	该应用运行后会监听用户通话，替换拨打号码，上传用户隐私信息，造成用户资费消耗和隐私泄露，建议卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 中存在安全漏洞 (CVE-2014-8439)	Adobe Flash Player 中存在安全漏洞。攻击者可利用该漏洞执行任意代码或造成拒绝服务（无效的指针逆向引用）。以下产品及版本受到影响：基于 Windows 和 OS X 平台的 Adobe Flash Player 15.0.0.167 及之前版本和 13.0.0.244 及之前版本，基于 Linux 平台的 Adobe Flash Player 11.2.202.406 及之前版本；Adobe AIR 15.0.0.249 及之前版本，基于 Android 平台的 Adobe AIR 15.0.0.252 及之前版本；Adobe AIR SDK 15.0.0.249 及之前版本；Adobe AIR SDK & Compiler 15.0.0.249 及之前版本。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.Zerber	此威胁是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）
		Trojan[Dropper]/MSIL.Aotoit	此威胁是一类可以释放恶意代码的木马家族。该家族样本由 AutoIt 脚本编写，该家族样本运行后释放 AutoIt 脚本执行工具及恶意脚本，之后使用工具调用恶意脚本。（威胁等级中）
		Trojan[Downloader]/Win64.Carberp	此威胁是一类可以下载恶意代码的木马家族。该家族样本基于 64 位系统编写，运行后连接远程服务器下载恶意代码并运行，可能会收集系统敏感信息并回传。（威胁等级中）

云存储将成为网络钓鱼攻击的新宠儿

Jai Vijayan / 文　安天公益翻译小组 / 译

近日，PhishLabs 指出，2016 年的数据显示，针对 Google 和 DropBox 等云存储服务提供商的网络钓鱼攻击将会很快超过针对金融机构的钓鱼攻击。

在威胁源采用的所有复杂的战术、技术和程序中，网络钓鱼仍然是 2016 年最受欢迎的攻击手段。

安全厂商 PhishLabs 在本周发布的网络钓鱼趋势报告中指出，2016 年与以往最大的区别是，网络钓鱼者不再一门心思地攻击金融服务机构，而是越来越倾向于攻击诸如 Google 和 DropBox 这样的云存储服务提供商。

在 2013 年，仅有 10％的网络钓鱼攻击针对云存储服务公司。但是在 2016 年，这一比例达到了约 22.5％，已经非常接近针对金融机构的攻击比例 23%。这意味着，用户今年可能会收到更多的钓鱼邮件，试图诱骗他们提供云存储的凭证。

PhishLabs 高级安全威胁研究员科瑞恩·哈索德 (Crane Hassold) 说：“在过去的四年里，针对云存储服务的网络钓鱼攻击数量激增。从最近的趋势来看，针对云存储服务的钓鱼攻击很可能会超过针对金融机构的钓鱼攻击，成为 2017 年钓鱼者的首要目标。”

至少到目前为止，几乎所有涉及云存储的网络钓鱼攻击都只针对 Google 和 DropBox。

很多针对云存储提供商的网络钓鱼活动使用了诱饵，声称已经与受害者分享了文档或图片，诱骗他们登录网盘账户进行查看。

此类活动使用的大多数钓鱼网页只是简单地复制了 Google，DropBox 和其他合法网站的网页。即使如此，“这类攻击仍然越来越受欢迎，这说明，钓鱼者能够成功地利用这些缺乏可信度的页面感染受害者。”哈索德说。

PhishLabs 分析了超过 17 万个域中的大约 100 万个钓鱼网站，以及该公司在 2016 年每个月处理的超过 7800 次钓鱼攻击，在此基础上编写了网络钓鱼趋势报告。其分析显示，网络钓鱼活动正在以惊人的速度增加。

举例来说，2016 年钓鱼网站的数量比 2015 年增加了 23％；针对金融服务、云存储 / 文件托管、网络邮件 / 在线、支付服务和电子商务网站的钓鱼邮件数量平均增长了 33％。

PhishLabs 确定了网络犯罪组织在 2016 年用于钓鱼活动的 976 个云存储服务，它们分别属于 568 家公司。

2016 年，钓鱼者的目标数据类型也大大扩展了。除了账户凭证和个人数据，钓鱼者还试图使用钓鱼诱饵获取金融、就业和账户安全数据，如安全问题的答案和母亲的婚前姓名。

在 2016 年，网络钓鱼仍然是最受欢迎的勒索软件传播方法，其目标包括最终用户系统，企业、政府机构、学校和关键基础设施的系统。

2016 年网络钓鱼威胁激增的一个原因是，越来越多的网站已经接受电子邮件地址作为用户名。

哈索德表示，电子邮件地址作为用户名使得钓鱼者更容易收集钓鱼网站上的所有电子邮件账户的凭证，他们无需再攻击电子邮件服务提供商。

“此外，由于越来越多的网络服务使用电子邮件作为主要凭证，钓鱼者可以对这些毫无戒心的目标执行密码重用攻击，从而大大增加利润。”哈索德说。

用于创建钓鱼网站的工具包或模板很容易获得，这些因素也加剧了这一问题。PhishLabs 的统计表明，目前有超过 29000 个钓鱼工具包 (包含模板)，它们模仿了超过 300 家公司的网站。许多工具包具备复杂的反检测机制，包括基于 IP 地址、HTTP 引用、主机名、白名单和阻止列表的访问控制措施。

哈索德指出：“关键的问题是，我们为网络钓鱼攻击大规模收集凭证创造了理想的条件。”

过去，钓鱼者专注于获取即时收益 (例如追踪和出售金融账户的凭证)；而现在，他们试图以最少的精力获取尽可能多的信息。

他们的目标是“在地下市场以更高的价格出售信息，或利用这些信息进一步攻击二级目标，从而增加其收益。”哈索德说。

原文名称	Cloud Storage：The New Favorite Target Of Phishing Attacks
作者简介	Jai Vijayan，一位经验丰富的技术记者和自由职业作家，目前担任 Computerworld 的高级编辑，研究信息安全和数据隐私问题。
原文信息	2017 年 2 月 7 日发布于《Darkreading》 原文地址 http://www.darkreading.com/attacks-breaches/cloud-storage-the-new-favorite-target-of-phishing-attacks/d/d-id/1328078
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《使用 Python 语言编写的远控家族 Seaduke 介绍》

近日，安天追影小组发现一个以 Python 脚本编写的远控类病毒家族 Seaduke，该家族样本使用 PyInstaller 打包程序将 Python 脚本转换为可执行文件，样本运行时会通过接收远程命令来执行上传本地文件、下载和安装恶意程序、卸载和删除本身等这些恶意行为。

经安天追影小组分析，发现本次分析的 Seaduke 恶意软件样本很大，有 3.16MB，其使用 PyInstaller 将恶意软件的相关功能 Python 脚本和所需的动态库等文件打包转换成一个 EXE 文件，并进行加壳。

恶意软件一旦被执行，就会在系统临时文件目录“%Temp%\”下释放多个 pyd 文件，以及一个执行 Python 脚本所需的动态链接库“Python27.dll”，并在系统启动目录“%UserProfile%\Start Menu\Programs\Startup”下释放快捷方式和修改注册表启动项，来完成自启动。在对 Seaduke 恶意软件的 Python 脚本进行分析时，发现其中有判别系统环境是 Windows 还是 Linux 的功能代码。

所以根据 Python 脚本的跨平台特性，可猜测 Seaduke 家族可能是一个跨平台病毒家族，对于这一点，我们会持续跟进和追踪。目标机器感染恶意软件后，其会与 C&C 服务器发送连接请求，等待远程指令，包含以下命令：

Autoload：在指定的位置安装样本
Migrate：迁移进程文件
Clone_time：修改文件属性时间
Download：下载文件
Execw：执行命令
Get：上传文件（加密）
Upload_to：上传文件（不加密）
B64encode：加密文件内容并返回
Eval：执行代码
Set_update_interval：设置请求时间间隔
Self_exit：停止运行样本
Seppuku：卸载安装样本

从远程命令看，恶意软件通过远程操控，可进行下载、安装、执行其他恶意软件，以及窃取、上传被感染机器的数据，加密和混淆网络通信数据。

Seaduke 家族是一个利用脚本语言和相应的转换工具来生成样本的，脚本语言包含快速开发、容易部署、可同已有技术集成、易学易用、动态生成和执行代码等特点，运用于恶意代码领域，将使得恶意软件开发更容易。

目前，安天追影产品已经实现了对该家族样本的检出。同时，安天将持续关注脚本类恶意代码，以更早、更好的应对此类威胁。

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，依据行为即可实现对上述木马程序进行有效检测，以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、美国软件交叉索引 (NSRL) 鉴定器、数字证书鉴定器、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、安全云鉴定器等鉴定分析。最终依据 BD 静态分析鉴定器、安全云鉴定器将文件判定为木马程序。

文件名	A25EC7749B2DE12C2A86167AFA88A4DD
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	3.16 MB
MD5	A25EC7749B2DE12C2A86167AFA88A4DD
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[RAT]/Win32.Seaduke.a
判定依据	安全云

◆ 运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认、IE6、Office 2007、Flash，WPS、FoxitReader、Adobe Reader

根据动态行为（默认环境）得出该文件具有以下行为：获取系统版本、填充导入表（疑似壳）、读取自身文件、获取计算机名称、获取 socket 本地名称、获取主机用户名称、连接网络、释放 PE 文件、获取驱动器类型、获取系统内存、独占打开文件、访问文件尾部、打开自身进程文件。

◆ 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	★★	填充导入表（疑似壳）	★★
读取自身文件	★★	获取计算机名称	★
获取主机用户名称	★	获取 socket 本地名称	★
释放 PE 文件	★	连接网络	★
获取驱动器类型	★	获取系统内存	★★
独占打开文件	★	打开自身进程文件	★
访问文件尾部	★		

报告地址：https://antiy.pta.center/_lk/details.html?hash=A25EC7749B2DE12C2A86167AFA88A4DD