安天周观察

主办：安天　2017 年 1 月 16 日（总第 73 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

海关总署署长、党组书记于广洲一行参观安天总部

近日，海关总署署长、党组书记于广洲，副署长、党组成员邹志武一行来到安天哈尔滨总部考察，并听取了关于我司最新发展状况和项目情况的汇报。

在展示厅内，安天负责人为考察组介绍了安天的发展历程、安天参与重大活动的网络安保支撑、安天总体规划以及近期在技术创新和专利技术方面取得的部分成果。同时，安天负责人向考察组展示了安天安全威胁感知捕获体系与可视化平台。最后，考察组详细了解了安天针对恶意代码和重大安全攻击事件所发布的分析报告和安天全线产品。

目前安天已经形成了由流量检测产品“探海”、终端防护产品“智甲”、威胁阻断产品“镇关”和深度分析产品“追影”组成的体系化威胁检测防护解决方案。并通过态势感知与监控预警平台对感知、分析产品的统一管理与业务分析，形成服务行业、地区级用户的整体能力。

海关总署作为国内较早实现信息化的政府部门，已经实现了高度办公自动化、无纸化。它的工作既涉及国计民生又接触海量信息，这对其网络安全要求较高，对威胁检测的挑战和难度较大。

安天针对海关总署网络面临的威胁提供全面的威胁检测和分析解决方案，使其网络在加快威胁响应速度、应对 APT 事件、安全事件追踪，提升检测深度等方面的能力得到大幅度提升。于广洲对安天所取得的技术成果给予了肯定，同时作为安天的用户，他也对安天提出了期望，希望安天坚定信心，加强技术创新，继续努力做好网络安全防护工作。

北京安天党支部组织全体党员召开专题组织生活会和开展民主评议党员工作

2017 年 1 月 9 日，北京安天党支部组织全体党员召开专题组织生活会，并对开展民主评议党员的工作进行了安排部署。

会上，北京安天党支部书记陈淑兰组织党员深入学习了习近平总书记在党的十八届六中全会上的重要讲话精神，解读了本次召开专题组织生活会和开展民主评议党员的相关要求。全体党员对照“四讲四有”合格党员标准以及本支部讨论制定的合格党员行为规范进行了批评与自我批评。会上还对经过公司党员选举，公司党支部报送，海淀园工委评选出的“优秀共产党员”行了表彰。

安天党支部全体党员表示，将认真对照、学习党章党规和“四讲四有”合格党员标准，以实际行动履行践诺，为构建“学习型、服务型、创新型”党支部贡献自己的力量，更好地发挥基层党组织战斗堡垒作用和党员先锋模范作用。

■ FDA 发布警告称 St Jude 生产的植入起搏器和心血管仪器存严重安全性问题

美国食品和药物管理局 (FDA) 近日发出警告称心血管设备生产商圣犹达医疗 (St Jude Medical) 的部分产品存在网络安全性问题，其生产的特定型号起搏器和心血管仪器产品极易被黑客侵入。2016 年 9 月，FDA 计划彻查心血管设备生产商 St Jude 的产品安全性问题。

FDA 指出，脉冲发生器 / 起搏器可以被黑客恶意修改，经过修改后黑客可以从植入的脉冲发生器中读取数据，并将数据发送到医院的服务器上。该产品非常容易遭到篡改，被篡改后容易引起植入的脉冲发生器中止工作，危及患者生命。（来源：https://www.easyaq.com/newsdetail/id/352733350.shtml）

■ Android 漏洞“启动模式”曝光 或致设备被窃听

近日，Android 曝光了“启动模式”漏洞。以往攻击者需要通过复杂的过程来入侵调制解调器达到监听通话的目的，但现在，IBM 团队已经证实了利用“启动模式”漏洞达到此类目的的可行性。好消息是 Google 已经修复了 Nexus 6/6P 智能机上的这一“高危漏洞”。

此前，攻击者可以通过 USB 连接，在启动过程中接管板载调制解调器，窃听电话和拦截移动数据包。CVE-2016-8467(CNNVD-201701-022) 是 IBM X-Force 安全研究人员发现的多个安全漏洞之一，“启动模式”漏洞利用被恶意软件感染的 PC（或任意电源适配器）来隐匿访问 USB 接口。（来源：http://www.cnnvd.org.cn/news/show/id/8076）

每周安全事件

类 型	内 容
中文标题	英特尔 CPU 的调试机制被发现允许攻击者接管系统
英文标题	Debugging mechanism in Intel CPUs allows seizing control via USB port
作者及单位	Roi Perez；SC Media
内容概述	近日，安全研究人员发布警告称，部分英特尔的新 CPU 含有调试接口 JTAG (Joint Test Action Group)，能通过 USB 3.0 端口访问，可被用于控制操作系统，执行现有安全工具无法检测的攻击。攻击者能利用调试接口绕过所有的安全机制，读取所有的数据，甚至可以通过重写 BIOS 使系统停止工作。 研究人员在近期举行的 33C3 黑客会议上讨论了此类攻击。研究人员 Maxim Goryachy 和 Mark Ermolov 称，这些工厂创造的硬件机制有其合法用途，如硬件配置的特定调试功能，但这些机制也给攻击者提供了机会，而执行此类攻击无需国家资源或特殊设备。
链接地址	https://www.scmagazine.com/debugging-mechanism-in-intel-cpus-allows-seizing-control-via-usb-port/article/630480/?utm_source=tuicool&utm_medium=referral

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.Npop.a[exp，sys] 2017-01-10	该应用程序安装后会隐藏图标，运行后会自动连网下载并静默安装未知应用，拦截并删除包含特定字符的短信，静默发送大量未知短信，建议卸载。（威胁等级高）
		G-Ware/Android.HijackBrowser.a[exp，rog] 2017-01-10	该应用程序会劫持浏览器频繁访问广告页面，造成用户资费消耗，建议谨慎使用。（威胁等级低）
		Trojan/Android.HiddenApp.s[rog，prv]2017-01-12	该应用运行后会非强制性申请设备管理器权限，并隐藏自身图标，获取并上传硬件信息，建议卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.emial.ec[prv，exp，fra]	该应用会伪装成其他应用，运行后会隐藏图标，后台会拦截用户短信并通过短信和邮箱转发短信内容，短信发送用户来电记录和地理位置信息，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.Downloader.db[exp，rog]	该样本会伪装成正常应用，运行后会不断置顶设备管理器，强制用户授权，后台会自动连网下载未知应用，会弹窗强制用户安装应用。造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.LockScreen.e[rog，exp]	该应用为勒索软件，会锁定用户屏幕，造成用户无法使用，并会要求用户添加指定 QQ 付费解锁，建议不要安装。（威胁等级高）
		Trojan/Android.Koler.g[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，以非法浏览色情为由置顶界面勒索用户付费，造成用户资费损失，建议不要安装。（威胁等级高）
		Trojan/Android.emial.ee[prv，rmt，exp]	该应用会伪装成正常应用，运行后会隐藏图标，接收远程指令，上传用户短信、通话录音、地理位置和截屏等隐私信息，静默安装守护进程子包，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.emial.ef[prv，exp]	该程序会伪装成银行证书类应用，运行后会隐藏图标，获取用户收件箱信息，拦截短信并上传到云端，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 无效索引远程执行代码漏洞 (CVE-2014-6334)	Microsoft Word 在分析经特殊设计的 Office 文件时未正确处理内存中的对象，会导致当前用户的上下文中存在远程执行代码漏洞。漏洞会允许攻击者执行任意代码，从而损坏系统内存。以下产品受到影响：Microsoft Word 2007 SP3、Word Viewer、Office Compatibility Pack SP3。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Zlob	此威胁是一种具有下载行为的木马类程序。Zlob 家族感染用户电脑后，会修改系统设置，在电脑中下载并执行多个恶意软件。该家族会伪装成 ActiveX 的视频编码诱使用户下载并安装，安装后，用户会收到伪装成微软警告信息的弹窗，提示用户系统中可能存在间谍软件，需要下载反病毒程序进行清除。在用户点击弹窗后，将下载实为木马的虚假反病毒程序。（威胁等级高）
		Trojan[Banker]/Win32.Banbra	此威胁是一种以窃取网络银行敏感信息为目的的木马类程序。该病毒会伪装成正常数据，以获取认证。该病毒利用各种途径，使黑客获得数字证书来伪造文件。该家族还会收集用户的机密信息，如网上银行详细信息和密码等，并会将窃取的数据远程发送给黑客。（威胁等级中）
		Trojan[Dropper]/Win32.Brpd	此威胁是一种具有捆绑行为的木马类程序。该家族会携带各种恶意软件，在用户电脑中安装并运行。（威胁等级高）

FireCrypt 勒索软件携 DDoS 组件来袭

Catalin Cimpanu / 文　安天公益翻译小组 / 译

近日，研究人员发现：名为 FireCrypt 的勒索软件家族会加密用户的文件，还会对硬编码在其源代码中的 URL 发起非常微弱的 DDoS 攻击。MalwareHunterTeam 发现了该勒索软件，与 Bleeping Computer 网站的劳伦斯·亚柏拉罕 (Lawrence Abrams) 一起对它的行为模式进行了分析。

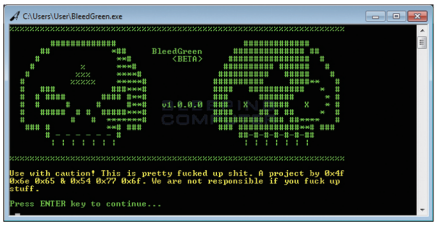
FireCrypt 是一个勒索软件构建套件

恶意软件通常从源代码编译而来，或使用自动化软件生成，该软件会针对每个攻击活动采用特定的输入参数生成自定义的恶意软件载荷。这种恶意软件载荷在业界被称为恶意软件构建器，通常作为命令行应用程序或基于 GUI(图形用户界面) 的工具。

FireCrypt 勒索软件的作者使用一个命令行应用程序，会自动化地将 FireCrypt 样本集合起来，因此，他不必再修改编译其源代码的大型 IDE(集成开发环境) 就能够更改基本设置。

FireCrypt 的构建器被称为 BleedGreen，它允许 FireCrypt 的作者生成一个独特的勒索软件可执行文件，并自定义该文件的名称，使用个性化的文件图标。与其他勒索软件构建器相比，它是一个非常低端的应用程序。类似的构建器通常允许敲诈者自定义更多的选项，例如接收赎金的比特币地址，赎金数额，联系人电子邮件地址等。

构建器除了将 EXE 文件伪装为 PDF 或 DOC 文件以外，还能对勒索软件的二进制文件稍作修改，以便在每次新编译时生成具有不同哈希值的文件。恶意软件开发人员常利用该技术创建难以被标准杀毒软件检测到的“多态恶意软件”。MalwareHunterTeam 指出：“构建器是非常基本的工具，它无法对抗真正强大的杀毒软件。”



FireCrypt 感染进程

FireCrypt 感染进程的实现取决于传播者是否能够成功诱骗用户执行生成的 EXE 文件。一旦受害者执行 EXE 文件，FireCrypt 将终止计算机的任务管理器 (taskmgr.exe)，并使用 AES-256 加密算法加密 20 种类型的文件。所有被加密的文件的文件名和扩展名都将附加后缀“.firecrypt”。例如，名为 photo.png 的文件将被重命名为 photo.png.firecrypt。

文件加密过程结束后，FireCrypt 会在用户的桌面上显示赎金要求。FireCrypt 几乎完全照搬 Deadly for a Good Purpose 勒索软件的赎金要求。Deadly for a Good Purpose 勒索软件于 2016 年 10 月被发现，当时其还处在开发阶段。只有当受害者的计算机日期是 2017 年及以后的时间时，其源代码才会启动文件加密进程。

相比 Deadly for a Good Purpose，FireCrypt 的赎金要求顶部没有“Deadly for a Good Purpose”的标识。但是，通过仔细检查 Deadly 的源代码，MalwareHunterTeam 发现这两个勒索软件使用相同的电子邮件地址和比特币地址，这说明两者之间存在密切的联系，FireCrypt 是在 Deadly 基础上重新编译的。

用垃圾文件填充硬盘的 DDoS 功能

显示赎金要求后，FireCrypt 并不会停止它的恶意行为。其源代码能够持续连接到一个 URL，下载该 URL 的内容并将其保存到 %Temp% 文件夹。如果用户没能发现此功能，FireCrypt 就会迅速在 %Temp% 文件夹下填满垃圾文件。同时，FireCrypt 勒索软件的当前版本能够下载巴基斯坦电信管理局的官方门户网站 (http://www.pta.gov.pk/index.php) 的内容。此外，所有受害者都将会被同时感染，勒索者会将他们的计算机联网，以参与 DDoS 攻击。

在编写本文时，研究人员还未找到解密被加密文件的方法。研究人员建议被感染但无法或不愿支付 500 美元赎金的受害者保留加密文件的副本，以待解密器的出现。

原文名称	FireCrypt Ransomware Comes With a DDoS Component
作者简介	Catalin Cimpanu，研究范围涵盖各种主题，包括数据泄露、软件漏洞、漏洞利用代码、黑客攻击新闻、暗网等。
原文信息	2017 年 1 月 4 日发布于《Bleeping Computer》 原文地址 https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/
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。

冬训营专题培训图文记录（节选）

为期两天的安天冬训营已经结束，第一天开放式技术报告带来了内容丰富的议题演讲，第二天的专题培训中安天各主线研发部门负责人分享了多个专题报告。现在，小编带您一起回顾专题培训中部分精彩的报告。

安天“下一代威胁检测引擎”

反病毒引擎的定义

传统的检测是围绕着输入对象的黑白判断展开的，采用特征检测、启发式扫描和其他决策方法，对输入对象是不是恶意代码以及是何种恶意代码做出判断进行输出。这就使攻击者可以通过免杀、0day 漏洞、碰撞构造等方式逃避检测。安天下一代威胁检测引擎，不是简单的把检测引擎作为判定器，而是进一步强化引擎的全对象识别和向量输出能力，辅以配套的后台知识和信誉积累，并将其转化为用户场景中可输出能力。通过大量向量提取输出和信誉标注，提升关联分析环节、支撑上层态势感知系统和工程师团队能力以及态势感知与综合决策能力。

面向新兴威胁的终端防护技术

安天智甲终端防御系统的特点

安天智甲终端防御系统是专为企业、政府、机构等业务网络研发的终端威胁安全防护产品，它以本地引擎和云查杀技术为基础，也支持未知程序的发现与防御；除具有传统反病毒产品功能外，还具有纵深防御能力以应对新兴威胁；对多种类型的终端进行统一管理，并可以持续扩展安全能力。

智甲面向政企用户网络安全需求，集成了安天自主先进 AVL 反病毒引擎；除了具备企业反病毒产品的标准功能外，还可以针对高级威胁 (APT) 进行全网威胁追溯和定点查杀；针对勒索者病毒等新兴威胁提供了面向终端的纵深防御能力；面向 ATM 和工控上位机等专用终端，智甲支持基于多种安全基线的白名单防御模式。同时智甲能够对 Windows、Linux 和国产系统提供有效防御并进行统一管理。

移动威胁对抗升级——人与机器思辨

报告分享了安天过去 5 年里移动引擎研发和工程化体系建设中的经验，对移动威胁对抗的本质以及其核心价值观进行了“术”和“道”层面的解读。随后从对抗中的人和机器，以及人和机器之间的各种关系的视角，对安全对抗背后的故事进行了思考和分享。通过这些思考，向观众做出了移动安全场景下“智者安天下”的产品和服务理念的解读。

关键威胁的持续追踪与网络监测

安天探海威胁检测系统 (以下简称探海) 在全流量元数据记录的基础上，利用安天下一代威胁检测引擎向量提取的能力，通过多标签联合筛选。探海辅助用户在海量数据中找到关键威胁，构建客户自有场景下的威胁持续追踪分析能力。通过标签聚合，可以实现对海量数据的降维；借助含有指示的标签，用户可以筛选构建自己关注的场景，减少在发现关键威胁信息过程中耗费的时间；配合安天引擎向量提取的能力，更可以建立独有场景下的专用规则。

基于沙箱的威胁情报输出

威胁情报具有防护、监控、取证、追溯作用，可用于 APT、DDoS、僵木蠕等领域。本地沙箱产出的威胁情报具有知识关联和本地独特性，在长尾的威胁情况下具有及时有效的组织防御价值。

安天本地化沙箱可以对样本进行分析获得样本黑白信息，这些信息包括样本的核心目的、样本属于哪种黑客攻击武器。沙箱输出可以检查威胁情报特征，这些特征具有上下文关联信息，包含丰富的知识。利用这些威胁情报可以第一时间对企业自身进行漏洞文档防护与网络监控终端取证。监管机构可以分析样本获取僵木蠕的 C&C，进行 DDoS 监控预警，对攻击者进行关联追溯等。

安天可视化的成长历程和自我批判

安天可视化团队经历的四个重要时期

安天可视化团队自 2012 年组建以来，经历了四个重要时期，在每个时期不同产品和需求的引导下，沉淀了不同阶段的成果。

报告对缺少操作性和可交互性的“地图炮”做了深入的反思和批判。安全可视化不应该停留在宏观上的、实时的和追求酷炫的展示手段，安全可视化要形成价值，必须能从宏观而及微观，是可操作的和可以实现有效的价值输出的。

冬训营的最后，安天创始人、首席技术架构师肖新光对本届冬训营做了总结，他表示，“今年安天冬训营的主要导向是要回归有效客户价值这个本质”，“安天举办冬训营的出发点是希望大家能在哈尔滨严冬的环境中，感受到网络安全所面临的压力与挑战”，“在历史机遇出现的时候，我们要能建立起自己的目标”，共同携手，铸就“冰峰屹立”。

(完整内容请关注微信公众号 antiylab)