安天周观察

主办：安天　2017 年 5 月 1 日（总第 85 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

黑龙江省委书记张庆伟莅临安天调研

4 月 18 日，黑龙江省委书记张庆伟在哈尔滨调研时，莅临安天。安天创始人、首席技术架构师肖新光及安天相关负责人为省委书记做参观引导，并进行了汇报。

在安天负责人介绍去年 4・19 网信座谈会及 5・25 总书记视察安天时的情景及总书记的嘱托时，张庆伟书记表示“要把总书记的嘱托转化为咱们创新创业的动力”。进入展示厅后，安天相关负责人沿总书记 5・25 视察路线向省委书记一行介绍了安天的发展历史、发展状况以及安天近年来在技术创新和知识产权方面取得的部分成果。展示了安天安全态势感知系统和可视化平台。张庆伟书记对安天创业以来各方面取得的成果表示肯定，并针对安天的发展规划，对重要的网络安全事件的发现上报、企业课题申报、员工工作状况等各方面问题的进行了询问。听到安天负责人回应员工对网络安全的态度上源自对行业的兴趣、热爱，以及爱国心的促使时，张庆伟书记郑重的说道，“你们不仅仅是员工，也是这方面的专家，贡献很大。”

参观结束后，张庆伟书记对安天的发展提出几点建议，他指出，企业要自主把握好技术方向，提高吸引力，聚集更多人才，建立起员工激励机制。同时，张庆伟书记也表示对于安天的发展，政府一定会直接关心、全力支持，帮助解决问题，各方要牢记总书记交代的使命、不忘企业自身的追求、结合政府部门的条件支持，协同促进黑龙江省科技创新和发展。

海淀区人民政府副区长李长萍一行视察安天

4 月 17 日，正值习近平总书记 4.19 主持召开网络安全和信息化工作座谈会并发表重要讲话一周年前夕，海淀区人民政府副区长李长萍、区经信办主任何建吾、区投促局副局长王春生及海淀园管委会服体处副处长王伟一行领导莅临安天视察，观看了安天产品和技术演示，听取了关于安天发展状况和产品应用等的汇报。

在产品展示中心，安天负责人为副区长一行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以及安天在技术创新和专利技术方面取得的部分成果，同时展示了安天安全态势感知系统，并对安天流量检测产品“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”作了讲解。

在汇报过程中，李长萍副区长始终严肃、认真地倾听安天负责人的介绍，并与安天负责人互动交流。

安天被授予“青年文明号”、青年就业创业见习基地

日前，哈尔滨团市委批复同意安天成立团总支部，并授予安天哈尔滨市级“青年文明号”称号及创建青年就业创业见习基地的资质。

在 4 月 12 日举行的揭牌仪式上，安天团支部书记首先向与会人员介绍了安天的发展状况及团总支部的建设现状，随后，团市委李娜副书记和安天相关负责人共同为市青年文明号和青年就业创业见习基地揭牌。

安天本身就是青年学子创业成长起来的高科技公司，此次揭牌仪式推动安天服务青年就业创业行动更进一步。

今后，安天将努力发挥公司优势，聚合社会资源，健全工作载体，发挥“青年文明号”示范带头作用，用实际行动为市“青年文明号”添彩，为广大青年学子和网络安全爱好者提供更多学习、工作的机会。

金融诈骗出新招：伪造达美航空支付邮件传播恶意软件

相关研究人员近期发现一起伪造达美航空支付确认邮件传播恶意软件、企图获取受害者银行账户信息的金融诈骗案。

研究人员表示，诈骗邮件并非像常规邮件那样提及航班信息，而是仅仅留有一个敦促用户快速点击的链接。

另外，如果用户仔细观察接收到的电子邮件就会发现地址栏中呈现的是 @deltaa 而非 @delta.com。

据悉，这宗诈骗案背后的整个逻辑是让受害者误认为有人通过盗取自身凭证购买机票，即受害者邮箱里会出现一张署有他人名称的电子收据。

在这种情况下，慌乱之中的受害者往往会在接到邮件后点击邮件中包含的所有链接，以便了解事件的来由及潜在开销。（来源：http://hackernews.cc/archives/9250）

一周简讯

- 英国医疗 CERT 发布勒索软件 Mole 预警
- 安全厂商找到勒索软件 XPan 变种破解方法
- FalseGuide 用手机构建移动僵尸网络
- 现代汽车移动应用存在远程利用漏洞
- 勒索软件 Locky 采用多层嵌套模式传播
- 监控厂商间谍软件 FlexiSPY 源码泄露
- 安卓后门 MilkyDoor 可以访问企业内网

安天 CERT 整理，详情请见 http://bbs.antiy.cn

每周安全事件

类 型	内 容
中文标题	NSA 泄露的恶意软件 DoublePulsar 已感染 3.6 万台设备
英文标题	Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs
作者及单位	Swati Khandelwal；The Hacker News
内容概述	近日，据外媒 BleepingComputer 报道，DoublePulsar 是由 Shadow Brokers 泄露的 NSA 黑客工具之一，现在该工具已被普通黑客使用，在全世界感染了超过 36000 台设备。 Shadow Brokers 黑客组织近期泄露了 NSA 方程式组织的一些工具，其中名为 DoublePulsar 的后门程序可利用部分 Windows 系统 (Windows XP，Windows Server 2003，Windows 7 和 8 以及 Windows 2012) 漏洞进行恶意代码注入及运行。由于此批工具可被世界各地的脚本小子及在线犯罪分子利用，全世界数十万暴露在互联网上的 Windows 计算机正在受到威胁。据多名安全专家的互联网扫描显示，该次事件可能影响数万 Windows 系统计算机。
链接地址	http://securityaffairs.co/wordpress/58129/data-breach/intercontinental-hotels-group-breach.html

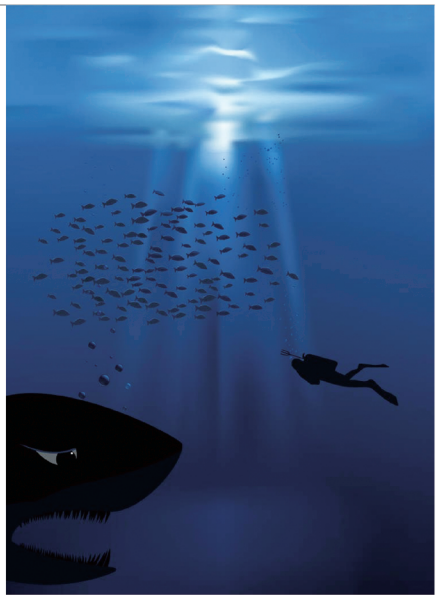
每周值得关注的恶意代码信息

经安天检测分析，本周有 8 个移动平台恶意代码和 5 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	新出现的样本家族	Trojan/Android.marswin.a[prv，rmt] 2017-04-24	该应用程序为间谍软件，运行后隐藏图标，获取 root 权限，若手机没有 root 则执行 root；获取远程服务器控制指令，窃取用户联系人、通话记录和地理位置信息等；执行通话录音、环境录音、拍照和截屏等操作，造成用户隐私泄露和资费损耗，影响手机系统稳定，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.SmsListener.p[prv]	该应用程序安装无图标显示，窃取收件箱短信，造成隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Marcher.c[prv，exp]	该应用程序启动隐藏图标，伪装成银行卡登录界面，窃取用户账号、密码，拦截短信、获取设备 ID 并上传，诱导激活设备管理器导致无法正常卸载，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.emial.fh[spr，exp，prv]	该应用程序启动获取设备 ID 等信息并发短信到指定号码，接收远程指令，读取手机通讯录并群发垃圾短信，造成用户资费消耗和隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.FakeFB.h[prv，fra]	该应用程序伪装成 Facebook 破解应用，运行后诱导用户输入 Facebook 账号和密码并短信转发到指定号码，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.HiddenApp.aa[exp]	该应用程序伪装 Google 应用，运行隐藏图标，激活设备管理器，跳转推广网页，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.HiddenAds.br[exp，rog]	该应用程序伪装成系统应用，运行时会隐藏图标，后台推送广告，造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.BankBot.c[prv，exp，rmt]	该应用程序伪装成其他应用，程序运行会请求激活设备管理器，隐藏图标，上传固件信息，访问指定网址，诱骗用户下载安装更新应用，利用银行相关钓鱼界面窃取用户银行卡账号密码相关信息；监听、拦截短信并上传短信，私自发送指定短信，造成用户隐私泄露和资费消耗。（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 内存损坏漏洞 (CVE-2016-7193)	当 Office 软件无法正确处理 RTF 文件时，Microsoft Office 软件中存在远程执行代码漏洞。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）
	较为活跃的样本	Trojan/Win32.Nemuco	此威胁是一类可以下载勒索软件的木马家族。该家族样本一般是 JS 编写的脚本，运行后连接远程服务器下载勒索软件并执行，加密用户文档来要求支付比特币解锁。（威胁等级中）
		Trojan[Exploit]/SWF.Angler	此威胁是一类木马家族。该家族因 Angler Exploit Kit 而得名。该家族的样本使用了 SWF 的漏洞对用户的设备进行感染，从而执行任意恶意代码。（威胁等级中）
		Trojan[Downloader]/Shell.Agent	此威胁是一类具有执行 shell 语句行为的恶意代码的家族统称。该家族的样本在执行后会利用 ShellExecute 等函数来执行特定的语句，对系统造成潜在危害。（威胁等级中）
		Trojan[Downloader]/Win64.BitMin	此威胁是一个下载器家族。该家族的样本是基于 64 位 Windows 平台的。该家族样本在执行后具有下载行为，在后台下载并执行其他恶意软件。（威胁等级中）

xDedic 市场数据对企业造成威胁

Kelly Sheridan / 文　安天公益翻译小组 / 译



xDedic 是暗网上的热门市场，它销售 RDP(远程桌面协议) 服务器的访问权限，帮助犯罪分子攻击政府和公司。

xDedic 是暗网上最大和最具破坏性的市场之一。六个月前，商业风险情报公司 Flashpoint 发现它拥有一个数据库，其中包含超过 8.5 万个组织的信息。

网络犯罪分子在 xDedic 市场上购买受感染的 RDP 服务器的访问权限，这样一来，他们就能轻松进入在线系统。RDP 是微软的专有协议，它允许用户通过网络连接到其他机器，使管理员能够远程控制服务器和 PC。

Flashpoint 研究总监维塔利·克雷莫斯 (Vitali Kremez) 表示，Flashpoint 监控 xDedic 市场至少两年了。该市场自 2014 年投入运营，在网络犯罪分子之间建立了很好的声誉，这些犯罪分子攻入企业的 RDP 服务器，然后在该市场上转售凭证。

克雷莫斯解释说，黑客通常先扫描网络，寻找连接到微软远程桌面协议的特定端口。在确定了具有开放端口的服务器之后，他们会通过暴力破解的方式来测试用户名和密码组合，直到找到匹配项。

一旦他们获得 RDP 服务器访问权限，就会在 xDedic 市场上销售访问凭证并更新管理员权限。任何购买凭证的人都能够进入企业网络，进而窃取数据、提升权限、启动外部攻击、部署勒索软件、植入恶意软件、操纵网络设置以及控制账户。

克雷莫斯指出，对于简短而弱效的服务器密码来说，黑客的暴力破解非常有效。但是，他们很难破解更长更复杂的密码。然而，即使服务器的凭证很强大，大型僵尸网络仍然可以帮助攻击者获得 RDP 服务器访问权限。

克雷莫斯解释了以攻击医疗机构而闻名的威胁源“The Dark Overlord”是如何利用 xDedic 数据库来执行攻击的。医疗机构经常被攻击，这是因为一旦犯罪分子能够访问开放的 RDP 服务器，就能够窃取有价值的数据。

“我们一直在调查针对医疗机构的攻击行为”，他继续说，“我们发现，很多医院被攻击的原因是其 RDP 服务器凭证泄露了。”

但是，医疗机构并非头号目标。

xDedic 数据库包含超过 8.5 万台服务器的信息，能够帮助分析人员了解黑客最喜欢攻击的行业。数据分析显示，最常被攻击的行业包括教育、医疗、法律、航空和政府。美国、德国和乌克兰是最常被攻击的国家。

克雷莫斯说：“教育机构是最不安全的，最容易受到伤害。”他指出攻击者能够很容易地通过暴力攻击进入大学网络。然而，大学和医疗机构都有信息共享社区，他们可以通过这些社区共享攻击信息，并改进其信息安全程序。

克雷莫斯认为，xDedic 的威胁还会继续增长，特别是在 Shadow Brokers 发布漏洞利用工具之后。如果犯罪分子继续开发工具包并利用这些漏洞，扩展对其他网络的访问权限，那么他们将会造成更大的伤害。他指出，虽然这些漏洞并非零日漏洞，但它们仍然是很危险的。

克雷莫斯建议企业不要将服务器连接到外网并采取适当的访问控制措施。虽然对技术人员和网络程序来说，将服务器连网更加方便，但这是很危险的，因为网络犯罪分子通常会暴力破解这些连网的 RDP 服务器的访问凭证。

他还建议采取密码预防措施。“经常更改密码，并使密码尽可能复杂。”他表示，“至少，这样能够阻止 xDedic 攻击者。”

原文名称	xDedic Marketplace Data Spells Danger for Businesses
作者简介	Kelly Sheridan，Dark Reading 的副主编。
原文信息	2017 年 4 月 25 日发布于 Darkreading 原文地址 http://www.darkreading.com/threat-intelligence/xdedic-marketplace-data-spells-danger-for-businesses--/d/d-id/1328721?
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《Cerber 勒索软件家族分析报告》

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，勒索软件 Cerber 的变种不断地更新，该家族也变得更加活跃。该勒索软件目前已将大版本号更新到 6，令人惊讶的是，从第一个版本到现在的版本 6，一共只用了一年左右的时间。

自 2016 年开始，采用了勒索软件即服务 (RaaS) 模式，名为 Cerber 的勒索软件开始爆发。攻击者在 2016 年下半年开始了频率极高的版本升级，仅在 8 月份就发现了 Cerber2 和 Cerber3 两个版本，而在 10 月及 11 月，Cerber4 和 Cerber5 相继推出，而进入 2017 年，Cerber6 面世。

勒索软件即服务 (RaaS) 是一整套体系，指从勒索到解锁的服务。勒索软件作者开发出恶意代码，通过在暗网中出售、出租或其他的方式提供给有需求的攻击者作为下线，下线实施攻击并获取部分分成，原始开发者获得大部分利益，在只承担最小风险的前提下扩大了犯罪规模。而采用这种服务模式的勒索软件越来越多地将目标放在了企业上。

Cerber 家族样本有多种传播方式，主要通过垃圾邮件和漏洞利用工具 Rig-V Exploit EK 传播，自 Cerber4 开始，它不再使用 Cerber 作为加密文件的后缀，而是使用 4 个随机字符。

同 Locky 一样，它也拥有本地化的功能，它会根据系统语言来显示不同的勒索警告文字。Cerber 采用 RSA2048 加密文件，拥有文件夹及语言地区的黑名单，在黑名单中的文件夹及语言地区均不能加密。样本加密的文件类型逐渐增加，现在已经从最初的几十种增加到数百种。在版本的演进中，Cerber 增加了结束常见数据库进程、判断本机时间等特性。

目前，安天追影产品已经实现了对 Cerber 家族样本的检出。

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：

文件被内部组件发现，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、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、静态分析鉴定器将文件判定为木马程序。

文件名	cerber4
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	426 KB
MD5	954D41391E39713E0E40F10E0848F2F3
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Zerber
判定依据	静态分析

◆ 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 2003、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：

填充导入表（疑似壳）、打开自身进程文件、读取自身文件、获取计算机名称、查找指定内核模块、关机、获取 socket 本地名称、创建特定窗体、获取驱动器类型、请求加载驱动的权限、获取系统版本、遍历进程、独占打开文件、文档篡改。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
填充导入表 (疑似壳)	★★	打开自身进程文件	★
读取自身文件	★★	获取计算机名称	★
关机	★	查找指定内核模块	★
创建特定窗体	★	获取 socket 本地名称	★
请求加载驱动的权限	★	获取驱动器类型	★
遍历进程	★	获取系统版本	★★
文档篡改	★★	独占打开文件	★

报告地址：https://antiy.pta.center/_lk/details.html?hash=954D41391E39713E0E40F10E0848F2F3