安天周观察

主办：安天　2016 年 9 月 26 日（总第 58 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

张效廉莅临安天参观指导
黑龙江省委常委、宣传部部长

9 月 22 日，黑龙江省委常委、宣传部部长、黑龙江省社科联主席张效廉一行到哈尔滨安天总部进行了实地考察。黑龙江省委网信办主任李耀东、哈尔滨市委常委、宣传部长张丽欣陪同参观。

安天相关负责人为考察组介绍了安天的发展历史和状况以及在技术创新和知识产权方面取得的部分成果，展示了安天安全威胁感知捕获体系和可视化平台。

张效廉部长对安天在技术创新和知识产权方面取得的成果表示肯定，并针对公司的业务特点，对电信诈骗、个人信息泄露等网络安全问题的解决方案进行了询问。同时，对安天的未来发展提出了几点建议，希望安天要保持自主创新的势头，提升自身发展的层次，把握机会，跟上势头，把企业做大做强，为实现黑龙江省更好更快发展作出贡献。

安天亮相 2016 国家网络安全宣传周

9 月 19 日 -25 日，以“网络安全为人民，网络安全靠人民”为主题的第三届国家网络安全宣传周在武汉举行。本次活动是我国网络安全工作中的一件大事，对于贯彻落实习近平总书记关于网络安全的重要讲话精神、维护广大人民群众在网络空间的利益、保障国家网络安全具有重要意义。

展会上，安天围绕“科普、生态、沙盘”三个主题，用电子图文科普计算机反病毒知识、用自主核心技术展示公司的生态价值、用乐高积木创意搭建了安全攻防沙盘，以兵棋推演的方式演练攻防对抗，备受大家关注。除武汉外，安天还同时在哈尔滨、深圳等地区参加了网络安全宣传周活动。

在 19 日上午的开幕式上，为表彰网络安全先进典型，经过中央有关部门和院士推荐、专家评审、公示，评选出网络安全杰出人才 1 名、优秀人才 10 名、优秀教师 8 名。安天创始人、首席架构师肖新光在内的十人荣获“2016 年网络安全优秀人才奖”。

习近平总书记在视察安天总部时曾说“你们也是国家队，虽然你们是民营企业”。现在安天已成长为国内威胁检测防御领域的技术领导厂商，感知能力覆盖全国，产品服务辐射全球多个国家地区。公司在重大网络事故和网络安全事件的响应中也发挥着关键作用，参加了十七大、十八大、2010 年起的两会、北京奥运会、2014 年 APEC 会议、抗战胜利 70 周年阅兵以及 G20 峰会等重大活动的网络安保工作，并获突出贡献奖。

安天当选黑龙江网信协会安全分会理事长单位

9 月 22 日，黑龙江省网络安全和信息化协会网络空间安全分会会员代表大会在哈尔滨市召开。黑龙江省委网信办、省公安厅、省网信协会以及省内外会员单位代表和专家共 100 余人参加会议。经会员代表大会表决，安天首席架构师肖新光任网络空间安全分会理事长，黑龙江省信息安全测评中心呼大永任分会秘书长。

黑龙江省网信办孙耀武副主任代表主管部门致辞。他强调，在网信事业发展的历程中，网络安全社会组织任重道远，特别是在我省经济社会爬坡过坎、滚石上山的关键时期，更要迎难而上，主动作为。要发挥好桥梁纽带作用，做发展网信事业的智囊团；要发挥好社会公益作用，做发展网信事业的生力军；要发挥好组织协调作用，做发展网信事业的先锋队。

安天首席架构师肖新光在发言时表示，黑龙江省地处东北老工业基地，有大量的关键基础设施和网络用户，能否搞好网络安全工作，是互联网 + 网络强省战略的重要基础。网络空间安全分会成立的目的是要把黑龙江省相关的机构、高校、网络安全企业和其他的非本省的安全企业驻省机构的能力有效聚集起来，实现习总书记在 5.25 视察安天时所说的“整体设计、加强合作，在相互学习，相互切磋，联合攻关，互利共赢中走出一条好的路子来。”。

每周安全事件

类 型	内 容
中文标题	门罗币 XMR 挖矿恶意软件正在利用希捷 NAS 设备进行传播
英文标题	Mal/Miner-C mining malware leverages NAS devices to spread itself
作者及单位	Pierluigi Paganini；Securityaffairs
内容概述	近日，据 Sophos 数据显示，2016 年上半年已经探测到了超过 170 万的设备感染 Mal/Miner-C 恶意软件，在受感染的系统中，大多数是在多个目录下运行该恶意软件多个副本的 FTP 服务器。 研究人员尝试使用扫描脚本匿名连接到 FTP 服务器中，试图找到存在写入权限的匿名 FTP。Sophos 专家还注意到，这类 FTP 服务器大多都运行在希捷 Central NAS 设备上。这种特殊的 NAS 设备可以提供一个不能删除或无法禁用的公共文件夹来共享数据，攻击者将恶意软件上传至文件夹中，在用户发现文件夹的第一时间运行恶意软件。此外，如果设备的管理员启用了通向设备的远程连接，这台设备就允许任何人从互联网接入。
链接地址	http://securityaffairs.co/wordpress/51131/malware/malminer-c-mining-malware.html?la=en

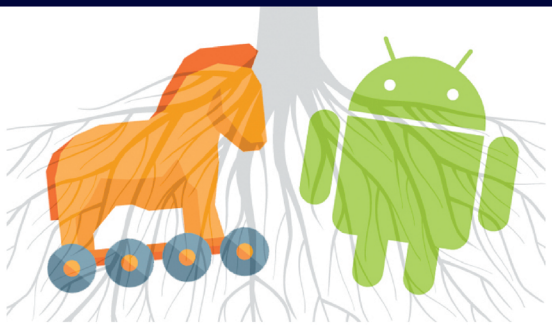
每周值得关注的恶意代码信息

经安天检测分析，本周有 10 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.Embassy.a[prv，spy]2016-09-20	该应用程序是间谍程序，后台窃取用户通讯录信息、位置信息、设备固件信息、安装列表信息、电子邮件账户等上传到远程服务器，建议立即卸载避免造成隐私泄露。（威胁等级高）
		G-Ware/Android.RogAd.a[rog，exp]2016-09-20	该应用运行会加载释放广告子包，匿名弹窗插屏广告，广告界面难关掉而且可能在无意操作中就下载，具有流氓行为，建议卸载。（威胁等级低）
		Trojan/Android.NzCopro.a[prv]2016-09-21	该应用监听手机 APP 安装消息，拦截未接短信，收集用户隐私信息，静默发送短信，造成用户隐私泄露、资费消耗，建议卸载。（威胁等级高）
		RiskWare/Android.Fakegle.a[prv，spy]2016-09-22	该应用伪装成 google，安装无图标。运行后监听 gmail 邮箱状态，获取用户联网信息，包含设备管理器监听行为，猜测为未开发完成程序。建议卸载。（威胁等级低）
		Trojan/Android.LevelDropper.a[rog，sys]2016-09-22	该应用运行会私自获取 root 权限，私自下载静默安装推送的应用，造成用户资费消耗。（威胁等级中）
		Trojan/Android.CJspy.a[prv，spy]2016-09-23	该应用程序为间谍件，运行后获取用户 SMS、MMS、照片、录像、联系人等各种隐私信息，造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.Ywjhdd.a[prv]2016-09-24	程安装无图标，触发启动，后台获取设备固件信息和收件箱信息上传到远程服务器，建议立即卸载，避免造成隐私泄露。（威胁等级高）
		Trojan/Android.koplayer.a[rog]2016-09-24	该应用启动会诱惑用户下载其他应用，并获取 root 权限安装应用，造成流量耗费，请谨慎使用。（威胁等级高）
	较为活跃的样本	Trojan/Android.Iop.c[rog，exp]	该应用程序伪装系统应用，本身无实际功能，后台联网下载提权文件，推送广告，建议立即卸载，避免造成资费损耗。（威胁等级中）
		Trojan/Android.Hqwar.b[prv，exp，rmt]	该应用启动后会隐藏图标，不断要求激活设备管理器，激活后会上传用户短信和联系人信息，执行远程指令，会造成用户隐私泄露，建议卸载该应用。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Mysql 远程代码执行 / 权限提升 (0day)(CVE-2016-6662)	它允许攻击者远程注入恶意设置到被攻击服务器的 Mysql 配置文件 (my.cnf) 中，导致更加严重的后果。该漏洞影响所有默认配置的 Mysql 版本分支 (5.7、5.6、5.5)，包括最新的版本，并可能被攻击者进行本地或者远程的利用。（威胁等级高）
	较为活跃的样本	Trojan[Dropper]/Win32.Small	此威胁是一种具有捆绑或释放其它恶意文件功能的木马类程序，该家族名称 Small 是根据样本大小特性命名的，该家族通常样本都很小。（威胁等级中）
		Trojan[Ransom]/Win32.Blocker	此威胁是一种赎金类木马程序。该家族入侵电脑后，会破坏电脑系统、损坏用户的文件，对用户文件加密使用户无法打开。此时黑客会向用户索要赎金并提供所谓的“密钥”，但用户支付赎金后仍然不能修复受损的文件。（威胁等级中）
		Trojan/Win32.Vobfus	此威胁是木马类程序。该家族运行后会修改注册表，阻止用户显示隐藏文件夹，连接网络下载其它恶意程序，该家族通常通过网络及可移动设备进行传播。（威胁等级中）
		Trojan[Backdoor]/Win32.Zegost	此威胁是一种后门类木马程序。该家族安装后注入系统进程，连接远程服务器，允许攻击者对被感染电脑进行控制。例如复制、下载和删除文件，捕捉屏幕截图，窃取用户敏感信息等。（威胁等级高）

安卓银行木马首次获得 root 权限

Chris Brook / 文　安天公益翻译小组 / 译



安卓银行木马背后的开发人员利用一个漏洞利用工具包帮助它获得 root 权限，由此强化了这种恶意软件。这是手机银行木马第一次试图获取 root 权限。

今年 2 月，研究人员发现了 Tordow 木马，但是很明显，攻击者在过去的几个月中对它进行了调整，帮助它获取 root 权限。

卡巴斯基实验室的恶意软件分析员 Anton Kivva 一直关注 Tordow 的演变，他在本周二凌晨发布了一篇博客，详细介绍了该木马的最新情况。

一旦应用程序中的恶意代码被触发，它就会下载其他恶意软件，其中包括一个漏洞利用工具包，它下载到系统文件夹中，帮助攻击者获取设备的 root 权限。就这样，攻击者就可以做任何想做的事情了。

该木马可以从被感染设备安装的浏览器 (无论是默认的安卓浏览器还是谷歌浏览器) 中窃取凭证，并窃听短信和电话。

通过访问浏览器的信息，攻击者可以收集保存在浏览器中的受害者银行账户信息，如登录名，存储的银行密码和 cookie。

更糟糕的是，具有超级用户权限后，攻击者可以从被感染的设备窃取任何文件，包括可能包含更多信息的照片，文档和文件。该恶意软件还能够重新启动设备，拨打电话，窃取联系人信息，安装和删除应用程序。

据卡巴斯基实验室介绍，大多数受害者在俄罗斯，他们也发现了该木马在乌克兰，中国和印度的一些活动。

攻击者将该木马植入热门应用程序的假冒版本中，如游戏《精灵宝可梦》(Pokémon Go)，即时通信软件 Telegram，以及欧洲社交网络应用程序 VKontakte。虽然受影响的应用程序并不在 Google Play 商店，但是攻击者依靠毫无戒心的用户通过第三方资源安装它们。

《精灵宝可梦》自今年 7 月上市以来很受欢迎，攻击者充分利用了这一点，将它集成到后门化的远程访问工具 (RAT) 并用它来传播勒索软件。卡巴斯基实验室的研究人员上周警告说，一款伪装为《精灵宝可梦》的恶意安卓应用程序进入了 Google Play 商店，安装在 6,000 台设备上，秘密获取了这些设备的 root 访问权限。

最近，一些漏洞诱骗用户授予攻击者安卓设备的 root 访问权限。

6 月份，谷歌发现其营应用程序商店里的一些程序自动获取设备的 root 权限，此后不得不删除了这些程序。当时，移动安全公司 Lookout 的专家发现了该恶意软件，认为它是移动威胁的最新和最具持续性的趋势之一。

本夏季，超过 90 万安卓设备遭到 Quadrooter 的感染，该漏洞允许攻击者绕过安卓 Linux 内核的减灾措施，并获取 root 权限。像 Tordow 一样，攻击者要想通过 Quadrooter 获得 root 权限，必须诱骗受害者下载一个恶意应用程序。

已经有越来越多的木马获得 root 权限并感染安卓设备的系统目录，但是对银行木马来说，该技术并非必要，因为它们通常可以通过多种途径窃取数据。Kivva 周二表示，考虑到越来越多的恶意软件试图获得 root 访问权限，银行恶意软件采用该方法只是一个时间问题。

Kivva 说：“最近，我们发现越来越多的恶意软件试图获得 root 访问权限。安卓银行木马做同样的事情只是一个时间问题。保护您的设备防御此类威胁非常重要，因为一旦它获得了 root 访问权限，几乎就无法删除了。”

原文名称	Android Banking Trojan First to Gain Root Privileges
作者简介	Chris Brook，卡巴斯基《安全周报 (Threatpost)》副编辑。
原文信息	2016 年 9 月 20 日发布于《安全周报 (Threatpost)》 原文地址 https://threatpost.com/android-banking-trojan-first-to-gain-root-privileges/120707/
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《HI-ZOR RAT 样本分析报告》

近日，安天追影小组整理安全事件时，针对 INOCNATION 行动中的 HI-Zor RAT 样本进行了分析。在 INOCNATION 行动中，攻击者采用了新的木马，在分析中观察到 HI-Zor 的字符串，将其命名为 HI-Zor RAT 木马。HI-Zor RAT 木马借用了许多其他恶意代码家族的相关攻击技术，例如：Etumbot 家族和 Ixeshe 家族的字符串混淆技术、Derusbi 家族的注册表篡改技术、Sakula 家族的攻击命令加密技术等。

经过分析可知 HI-ZOR RAT 样本由 Microsoft Visual C++ 6.0 平台编写，该样本为 DLL 文件，是 HI-Zor RAT 木马的核心功能模块。其通常被用作在感染主机中，并通过注册为服务项来响应攻击命令，并达到攻击者长期控制目的。HI-Zor RAT 木马的主要核心功能为：进程执行功能模块、反向连接 shell 功能模块、文件管理操作功能模块、上传文件功能模块、下载文件功能模块、自我更新和卸载功能模块。通过功能模块可以看出该木马为典型的远控木马病毒，通过感染目标，注册自身功能模块为系统服务项，对目标进行长期的控制以及窃取相关文件。

HI-Zor RAT 木马在通信方面主要使用 HTTP 协议的方式，通过发送类似 POST/ 1004122437VICTIM.1a53b0cp32e46g0xxxx HTTP/1.1，这样极具隐藏性的 http 数据包，来发送感染主机的配置信息。HI-Zor RAT 木马通过异或加密的方式修改配置信息字符串，来防御杀软的查杀和恶意代码工程师的分析。同时 HI-Zor RAT 木马采取了，篡改注册表键值的恶意代码常用的自启动方式。

通过对 HI-Zor RAT 样本分析，远控类木马的攻击强度和攻击频率仍然要求我们有足够的重视，并进行广泛的相关样本搜集和分析工作来提高自身的防御能力，从中总结出合理的分析解决方案来维护用户安全。安天追影小组针对此类木马建议网络使用者，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，针对可疑的文件或在遭到感染时及时寻求专业的技术支持，来保证系统的持久安全和维护财产数据安全。目前，安天追影产品已经实现了对该类样本的检出。

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，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：

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、YARA 自定义规则鉴定器、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 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木马程序。

该文件具有以下行为：获取系统版本、查找指定内核模块、获取系统内存、独占打开文件、获取计算机名称、疑似桌面控制。

文件名	75D3D1F23628122A64A2F1B7EF33F5CF
文件类型	BinExecute/Microsoft.DLL[:X86]
大小	22 KB
MD5	75D3D1F23628122A64A2F1B7EF33F5CF
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[RAT]/Win32.HI.ZOR
判定依据	动态行为

◆ 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

◆ 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	★★	查找指定内核模块	★
获取系统内存	★★	独占打开文件	★
获取计算机名称	★	疑似桌面控制	★

◆ 运行环境

操作	文件路径
新建	c:\windows\prefetch\ntosboot-b00dfaad.pf
新建	c:\windows\prefetch\copyfile.exe-09a9c969.pf
新建	c:\windows\prefetch\cmd.exe-087b4001.pf

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=75D3D1F23628122A64A2F1B7EF33F5CF