安天周观察

主办：安天　2016 年 2 月 22 日（总第 28 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布 2015 移动安全年报

近日，安天 AVL Team 发布了《2015 移动安全年报》，以恶意代码为基础视角，结合过去安全形势的演变历史，通过对 2015 年新案例的观察，以观点的方式来组织内容，用威胁的概念表达归纳了 2015 年的安全事态和趋势。

不堪重负的数据统计。2015 年，恶意样本的绝对数量和占比在整体环境放缓的情况下仍在快速提升。通过对 TOP10 家族统计数据，可以发现以色情应用、广告推送等为代表的恶意家族占比较大，这表明恶意代码通过和其他传统黑色产业合作，已经获得新的盈利空间和生存模式。

全面泛化的安全威胁。由于移动生态环节中的一些安全脆弱点，导致了威胁的频发和泛滥。未来安全趋势极大可能是被多个移动生态环节的安全事件所左右。这些安全事件标志着安全攻防已经不单单是暗流涌动，而是有愈演愈烈的趋势。移动生态的多个环节都面临着愈加明显的安全威胁，安全环境也变得日益复杂。

更具针对性的威胁形态。2015 年，移动威胁事件向着针对性攻击威胁发展，攻击者开始有意识的向特定范围的受害者，或者特定的用户群体进行攻击，甚至会出现针对特定企业或组织，特定地域范围的攻击。攻击者还可以通过掌握的通讯录等隐私信息，进一步升级攻击威胁，将具有群体针对性的威胁升级为个体威胁，从而提高威胁的准确性和侵略性。

持续扩大的威胁攻击面。2015 年，威胁的攻击面在持续扩大，iOS 安全受到考验，IoT 威胁攻击逐渐摆脱概念。虽然一些问题，仅仅还处在了解和探索阶段，但随着物联网的发展，智能设备逐渐开始渗透生活各个方面，突然大面积爆发某个安全事件是非常有可能的。

2016 移动安全威胁趋势。2016 年，面对威胁精确化和离散化的现状，进一步加强用户侧对威胁的感知能力，可能是安全厂商的必由之路。通过威胁情报的分析、加工和分享，从而对威胁进行准确定性、定位、定量。通过这样有针对性的服务，来满足和解决特定用户群体所面临的特定安全威胁，并向用户提供切实有效的解决方案，这样的体系或许是未来的发展方向。（全文地址：http://blog.avlyun.com/）

安天即将发布乌克兰电力系统遭受攻击事件综合分析报告单行本

2015 年 12 月 23 日，乌克兰国家电力部门遭受到恶意代码攻击，安天、四方继保、复旦大学三方在该事件后，建立了联合分析小组。根据对整体事件的跟踪及分析，联合分析小组推测目前所披露的大部分样本并不一定与该事件有关，而关于“KillDisk”组件直接导致断电的说法也并不科学。

近日，安天将联合分析小组的研究成果汇编成册，即将发布《BLACKENERGY 组织针对乌克兰电力系统攻击事件分析报告》单行本。

安天发布《首例具有繁体中文提示的勒索软件 LOCKY》报告 （见四版）

新年新气象　安天年味浓

每年新春之际，编写原创春联已成为安天传统的迎新方式之一。这些载有深深寓意和美好期盼的春联，记录了安天一步步地成长与发展。

此外，安天春节后的开工习俗也是年味十足。开工当日放一挂红红火火的鞭炮，既褪去了休假时的懒散，也热热闹闹地翻开了崭新的一页。喜气洋洋的开工红包更是带来了新年新气象，期盼安天人在新的一年里携手前行，共创佳绩。

2016 丙申年春联

安天奋起
智甲追影溯源　为君小心守护
引擎镇关探海　看我大圣归来

◆ 智甲：安天企业级终端防护产品，采用白名单 + 安全基线模式。
◆ 追影：安天威胁鉴定产品，集本地化沙箱动态分析与深度静态检测能力于一体。
◆ 引擎：安天 AVL SDK 恶意代码检测引擎。
◆ 镇关：安天威胁阻断产品，可以与安天威胁情报中心有效互动。
◆ 探海：安天威胁检测系统，支持千兆和万兆平台的载荷还原、检测、追溯。

每周安全事件

类 型	内 容
中文标题	尽快修复：利用恶意 DNS 服务器可劫持大量的 Linux 应用程序
英文标题	Patch ASAP：Tons of Linux apps can be hijacked by evil DNS servers，man-in-the-middle miscreants
作者及单位	Iain Thomson，The Register
内容概述	据了解，由于 GNU C 库 (glibc) 中存在一个严重漏洞，黑客可劫持大量的 Linux 应用程序。攻击者只需要点击一个链接，或者与目标服务器建立一条连接，就能够远程执行任意代码，犯罪分子便可以窃取密码，监视用户的操作行为，而且还可以尝试获取目标主机的控制权限。任何使用了 glibc 的联网软件都将有可能受到攻击。 恶意 DNS 服务器可能会在接收到查询请求时，返回大量的信息，在其返回的信息中附带 glibc 的漏洞利用代码。攻击者就可以利用这些攻击代码来入侵 Linux 应用，或者尝试接管整个系统。
链接地址	http://www.theregister.co.uk/2016/02/16/glibc_linux_dns_vulernability/

每周值得关注的恶意代码信息

经安天检测分析，本周 10 个移动平台和 4 个 PC 平台的恶意代码家族值得关注

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.jeini.a[fra，exp] 2016-02-15	该应用运行会请求激活设备管理器，隐藏图标，私自向用户联系人发送诈骗短信、监听短信、拦截短信并自动回复，造成用户资费消耗，建议及时卸载该程序。（威胁等级高）
		Trojan/Android.locseand.a[prv，rmt，fra] 2016-02-15	该应用程序伪装正常程序，无实际功能，诱导用户点击后会隐藏图标，后台执行联网上传联系人、短信箱、通讯录、地理位置等隐私信息，还含有拍照、通话录音功能，会给用户造成隐私泄露，建议及时卸载该程序。（威胁等级中）
		Trojan/Android.rtpkg.a[pay，sys] 2016-02-16	该应用程序伪装成系统程序，安装无图标，运行释放恶意子程序，检测杀软，后台联网获取配置信息，安装卸载指定程序，发送付费短信，还含有风险代码段，会给用户造成资费消耗，建议及时卸载该程序。（威胁等级中）
		Trojan/Android.Asacub.a[prv，rmt，exp] 2016-02-17	该应用伪装成正常应用，运行后激活设备管理器，隐藏图标，上传手机固件信息，sim 卡信息和手机号码，同时获取远程指令，根据指令会实现获取联系人、地理位置、程序列表信息、锁屏、开启摄像拍照、发送短信等功能，并会拦截屏蔽短信，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.wanda.a[prv，exp] 2016-02-18	该程序伪装成系统应用，诱导用户激活设备管理器，后台通过邮件窃取用户隐私、通过短信向联系人传播恶意链接，建议立即卸载，避免造成隐私泄露及资费损耗。（威胁等级中）
		Trojan/Android.pathcall.a[prv，fra，spy] 2016-02-18	该应用伪装成正常应用，运行后激活设备管理器、隐藏图标；后台获取用户 Facebook、gmail 和 WhatsApp 等社交应用聊天记录并上传；监听短信，获取短信和通话记录上传；而且会私自录音并上传，造成用户隐私泄露，建议卸载。（威胁等级高）
	较为活跃的样本	AdWare/Android.Niomin.a[ads]	该程序包含 Niomin 广告件，为 2048kg 平台的广告件，通过通知栏、弹框、创建快捷方式推送广告，可能造成资费损耗，请谨慎使用。（威胁等级中）
		AdWare/Android.skymobi.a[ads]	该程序包含冒泡 (skymobi) 开放平台的广告 sdk，运行时会获取手机固件信息，推送应用更新包和广告，可能会造成一定的流量消耗，建议谨慎使用。（威胁等级低）
		AdWare/Android.gmobi.a[ads]	该应用包含 gmobi.a 推送 sdk，运行后会获取手机固件信息和地理位置，推送应用更新包和广告，可能会造成用户资费损耗，请谨慎使用。（威胁等级低）
		AdWare/Android.yiipol.a[ads]	该应用包含 yiipol.a 广告插件，会以横幅、滚动形式展示广告，运行时会获取手机固件信息，请谨慎使用。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 对象处理远程代码执行漏洞 (cve-2011-0611)	Adobe Flash Player 是一款非常流行的 FLASH 播放器。它在对象类型的处理上存在远程代码执行漏洞，由于某个对象方法在被引用时没有正确识别对象的类型，导致远程攻击者可以利用此漏洞通过诱使用户访问包含恶意 SWF 文件的网页，在用户系统上执行任意指令，从而完全控制受影响的系统。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.Locky.a	此威胁是一种木马类勒索软件。它通过垃圾邮件进行传播。运行后会对系统内上百种文件格式进行加密。并弹出“重要資訊”图片，用户付款后才能进行解密文件。（威胁等级高）
		Trojan[Downloader]/Win32.Genome.aec	此威胁是一种木马类下载程序。运行后链接网络下载配置文件，查找系统中装有的游戏然后判断是否在配置文件中，有则下载此游戏盗号程序。（威胁等级中）
		Trojan[Backdoor]/Linux.Gafgyt.f	此威胁是一种木马类后门程序，运行在 linux 平台，主要功能为 DDOS 攻击、更新和下载等。通过扫描 SSH 弱口令进行传播。（威胁等级高）

美国情报机构负责人：

我们可能会利用物联网进行监控

Spencer Ackerman，Sam Thielman/ 文　安天公益翻译小组 / 译

近日，美国情报机构负责人第一次承认，美国情报机构可能利用新一代智能家用设备来提高他们的监视能力。

随着越来越多的设备连接到互联网并彼此连接，物联网为消费者提供了更大的便利。但是，随着家居计算不再局限于笔记本电脑、平板电脑和智能手机，专家警告说，汽车、洗碗机和报警系统等的安全功能远远落后。

在华盛顿智库会议中，国家安全局局长，海军上将迈克尔·罗杰斯说，现在是时候考虑将家居设备变得“更具防御性”了，但他没有说明越来越多的物联网设备数量和种类会为情报机构提供什么机会。不过，美国国家情报总监詹姆斯·克拉珀在提交给参议院的美国威胁评估证词中则更为直接。

“今后，情报部门可能会利用物联网进行识别、监视、监控、定位、跟踪，或者访问网络或用户凭证。”詹姆斯·克拉珀说。

克拉珀没有指出通过智能家居设备进行监控的具体情报机构。但是安全专家认为美国和其他监控机构将会拦截新连网设备发出的信号，就像他们拦截手机信号那样。业余选手们已经能够很容易地破解硬件；计算机程序员约翰·马瑟利的搜索引擎 Shodan 能够检索数千个不安全的连网设备。

在线威胁再次问鼎美国面临的“全球威胁”清单，紧随其后的是低强度恐怖主义。克拉珀承认家居连网设备的监控可能性，这对美国官员来说是很罕见的。但是，在 2012 年的一次演讲中，时任中央情报局局长戴维·彼得雷乌斯称物联网监控具有“转型意义 …… 特别是对秘密谍报来说”。

在对参议院军事委员会和情报委员会的证词中，克拉珀支持俄罗斯、中国、伊朗、朝鲜和伊斯兰国正在蓬勃发展网络间谍、造谣、盗窃、宣传和数据销毁能力。他警告说，随着这些国家“提高进攻性谍报能力、使用代理服务器和创建秘密组织”，美国正确追溯这些行动的能力可能会降低。

克拉珀认为，美国的对手已经超越了其网络能力：“俄罗斯和中国仍然拥有最先进的网络项目。”

白宫的新网络安全举措于近日揭幕，旨在增强非传统连网家居设备的安全性。它责成国土安全部“测试和认证物联网设备”。它没有讨论美国的网络安全和监控重点之间的紧张关系。

根据哈佛大学伯克曼互联网与社会中心发布的一项研究，连网家居设备是一个潜在的宝库，情报机构能够利用它们以不引人注目的方式来监听和监视目标。研究发现，以物联网为代表的信号爆炸式增加会压倒用户的任何隐私利益（商业加密方法），克拉珀在其证词中也再次表示，加密方法的增加对“情报收集带来负面影响”。

该报告的作者列举了 2001 年的一个案件，联邦调查局曾试图强迫一个制造汽车应急通信硬件的公司协助内华达州特工监听一个客户的汽车对话。2015 年 2 月，新闻报道显示，三星“智能”电视的麦克风 “一直开启”，以便接收任何指令音频。“执法和情报机构可能开始要求三星、谷歌、美泰、Nest 或其它连网设备厂商推广更新或翻转数字交换机，以便拦截目标的通信。”作者写道。

原文名称	US intelligence chief : we might use the internet of things to spy on you
作者简介	Spencer Ackerman，《卫报》驻美分支的国家安全方面的编辑，是《连线杂志》前自身作家。 Sam Thielman，《卫报》驻美分支的科技领域的作家。
原文信息	2016 年 2 月 9 日发布于《卫报》，原文地址 http://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper
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《首例具有繁体中文提示的勒索软件 LOCKY》

近日，安天 CERT 发现一款新的勒索软件家族，名为“Locky”，它通过 RSA-2048 和 AES-128 算法对 100 多种文件类型进行加密，同时在每个存在加密文件的目录下释放一个名为 _Locky_recover_instructions.txt 的勒索提示文件。经过分析发现，这是一类利用垃圾邮件进行传播的勒索软件，是首例具有繁体中文提示的勒索软件。

样本行为

1. 运行样本后，勒索软件文件会自复制为 *\temp\svchost.exe，运行并创建进程。

2. 同时，其会删除自身样本文件。另外并注册 *\temp\svchost.exe 为系统启动项，但在其后完成所有行为后会删除该文件，同时注册表信息也被删除，即并未实现自启动的功能。

3. 勒索软件进程 svchost.exe 会遍历系统中的所有文档类型文件，并进行加密，根据勒索提示文件获悉其是通过 RSA-2048 和 AES-128 暗碼進行了加密。并且在每个目录下面释放一个勒索提示文件 _Locky_recover_instructions.txt，来说明如何支付和解密流程。其中每个受害者都有一个个人识别 ID。

4. 完成加密操作后，勒索软件进程会删除自身进程以及相应的文件和注册表项。

5. 在对其网络通信行为进行分析过程中，会发现其会访问一个乌克兰 IP 地址，该网址目前无法打开。

总结

通过目前的分析来看，勒索软件“Locky”的功能与之前分析的勒索软件的功能基本一致。勒索软件能给攻击者带来巨大的收益，因其使用比特币进行交易，所以很难追踪；一旦用户感染了勒索软件，只能付费进行解密或是丢弃这些文件。安天提示广大用户，即使支付赎金也不一定能保证可以完全恢复被加密的文件。防止数据被加密，更应该注意勒索软件的防御，养成良好的上网使用习惯，不要轻易执行来历不明的文件。

“Locky”和其他勒索软件的目的一致，都是加密用户数据并向用户勒索金钱。与其他勒索软件不同的是，它是首例具有繁体中文提示的勒索软件，这预示着勒索软件作者针对的目标范围逐渐扩大，勒索软件将发展出更多的本地化版本。安天预测，今后中国将受到更多类似的勒索软件攻击。所以，如何防御勒索便成为保卫网络安全的重要任务之一。目前安天智甲已经实现了对该勒索软件的检测。（报告原文：http://www.antiy.com/response/locky/locky.html）

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、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。

暂时依据动态行为鉴定器将文件判定为木马程序，正在等待美国软件交叉索引 (NSRL) 鉴定器进行分析。该文件具有以下行为：仿冒 SVCHOST；安装输入法；根据进程名称复制文件；连接网络；获取计算机名称；获取 socket 本地名称；填充导入表（疑似壳）；释放 PE 文件；获取驱动器类型；增加 run 自启动项；独占打开文件；文档篡改；打开自身进程文件；获取主机用户名称。

文件名	17c3d74e3c0645edb4b5145335b342d2929c92dff856cca1a5e79fa5d935fec2
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	180 KB
MD5	FB6CA1CD232151D667F6CD2484FEE8C8
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	动态行为

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
仿冒 SVCHOST	★★★★	安装输入法	★★★
根据进程名称复制文件	★★★		

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
连接网络	★	获取计算机名称	★
获取 socket 本地名称	★	填充导入表（疑似壳）	★★
释放 PE 文件	★	获取驱动器类型	★
增加 run 自启动项	★	独占打开文件	★
文档篡改	★	打开自身进程文件	★
获取主机用户名称	★★		★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=FB6CA1CD232151D667F6CD2484FEE8C8