安天周观察

主办：安天　2016 年 4 月 18 日（总第 36 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加“打击治理电信网络新型违法犯罪”研讨会

4 月 14 日下午，由中国计算机学会计算机安全专业委员会和中国信息产业商会信息化与首席信息官分会联合主办的“打击治理电信网络新型违法犯罪研讨会”在北京召开，安天、360 等安全企业参加了会议。

会议列举了对网络诈骗犯罪的调研和电信诈骗案例，提出了打击治理电信网络新型违法犯罪的措施，以及就如何建立打击治理电信网络新型违法犯罪应急防范体系进行了讨论。安天安全研究与应急处理中心（安天 CERT）负责人李柏松在会上作了发言，他针对打击电信诈骗的预警提出两点建议：

1）可以由公安和有关部门牵头，增设电信诈骗短信举报平台，如公开的微信公众号等，便于大家举报和及时处理；

2）接收到举报信息后，联动相关安全企业，建立分析、预警信息的处置；然后可提交相关部门（如 CNCERT）进行处置，打断传播服务器、远控手机，定位嫌疑人，最终破获案件。

当前，电信网络新型违法犯罪已成为突出问题。今年 3 月 7 日，安天移动安全团队追踪破获了一起电信短信诈骗钱财案件，在有效时间内，帮助失主成功追回损失钱财。目前，电信网络犯罪呈高发事态，诈骗手段和方法不断翻新，作为用户，应该提高警惕，慧眼识骗；作为安全厂商，安天会积极配合公安等相关部门，发挥技术优势，严厉打击治理电信网络新型违法犯罪。

一周简讯

◆ 德克萨斯地区 20 所院校遭受勒索软件攻击 2.5TB 数据被加密。

◆ 勒索软件 CryptoHost 家族使用 RAR 密码保护机制加密文件。

◆ 研究者警告：蠕虫式勒索软件（cryptoworm）时代即将到来。

◆ 银行木马变种 Atmos 活跃 曾被勒索软件 Teslacrypt 使用。

◆ 研究人员发布破解工具：勒索软件 Petya 加密文件可被解密。

◆ 瑞典军方发现服务器被黑 曾在 2013 年被用于攻击美国银行。

◆ iOS 再现 1970 变砖漏洞 由假 WIFI 和 NTP 服务器触发。

（安天 CERT 搜集整理，详见：创意安天论坛 http://bbs.antiy.cn/forum.php）

BillGates Linux 僵尸网络被用于发动大规模 DDoS 攻击

安全研究人员称，地下网络犯罪分子在过去半年的时间里，实施了利用 BillGates Linux 僵尸网络发动攻击流量超过 100Gbps 的大规模 DDoS 攻击。BillGates 恶意程序是针对 Linux 服务器的一种相对有历史的恶意程序家族，它可以将感染的服务器连接起来创建一个僵尸网络。BillGates 僵尸网络支持发动 ICMP 洪水、TCP 洪水、UDP 洪水、SYN 洪水、HTTP 洪水和 DNS 反射洪水攻击。安全研究人员还指出，以往部署 XOR 僵尸网络的网络罪犯最近也开始切换到 BillGates 僵尸网络了。（文章来源：http://www.easyaq.org/info/infoLink?id=370307771）

Apple iMessage 曝新漏洞，黑客可远程浏览全部聊天记录

近日，Apple 解决了一个位于其消息应用 iMessage 中的漏洞（CVE-2016-1764），这个漏洞早在半年之前就被发现并上报给了 Apple，笔记本电脑与台式机均受该漏洞影响。该漏洞是通过社工手段，欺骗用户点击一个恶意链接，当用户点击后攻击者就可以浏览用户的聊天记录，包括视频和照片。这是一个应用层漏洞，攻击者通过利用 OS X 消息客户端远程获取所有以明文保存的信息内容及附件。（文章来源：http://securityaffairs.co/wordpress/46272/hacking/apple-imessage-flaw.html）

亚马逊在售商品已感染恶意软件

广大用户请注意，即便是亚马逊商城所售的商品中也有可能会存在恶意软件，这一令人感到恐慌的事实是由安全研究专家 Mark Olsen 所发现的。当时，Olsen 正在浏览一款户外监控摄像头，但当他登录进设备的 web 管理页面之后，他发现摄像头的信号输入接口并没有提供常见的控制选项。在对代码进行了审查之后，他发现在 web 管理界面的 iframe 框架中，包含有一个可疑的主机名。在 Google 中搜索了一番之后，他发现这个域名是一个曾用于网络欺诈活动（还包括恶意软件攻击）的恶意域名。Olsen 在报告中说到：“我们所提到的这一恶意软件并没有那么神秘，我们只需要利用 Google 来进行一些简单的搜索，我们就能得到大量关于这个恶意域名和恶意软件的信息。”（文章来源：http://securityaffairs.co/wordpress/46170/malware/amazon-products-infected-with-malware.html）

每周安全事件

类 型	内 容
中文标题	黑客组织攻击叙利亚政府网站 曝光 43GB 数据
英文标题	Syrian Government Hacked，43 GB of Data Spilled Online by Hacktivists
作者及单位	Catalin Cimpanu；SOFTPEDIA
内容概述	近日，黑客组织 Cyber Justice Team（网络正义小队）在 MEGA 文件托管服务平台上，上传了 10GB 来自叙利亚多个政府以及私营网站的压缩数据，解压后可达 43GB。另外，该组织还在 PasteBin 上传了来自叙利亚国家网络服务机构一台 Linux 服务器中的密码文件。安全分析师对来自 55 个不同网站域名的 38,768 个文件夹和 247,477 个文件展开了分析。在这 55 个域名中有 25 个属于政府网站（.gov.sy），两个为 .org.sy 域名，一个为 .com.sy 域名，其余则都是 .sy 域名。Cyber Justice Team 在 Twitter 表达了这次网络攻击的立场 —— 反对 ISIS、反对阿萨德政权，并称他们是“叙利亚人民的杀手”。
链接地址	http://news.softpedia.com/news/syrian-government-hacked-43-gb-of-data-spilled-online-by-hacktivists-502765.shtml

每周值得关注的恶意代码信息

经安天检测分析，本周 9 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	G-Ware/Android.plzll.a[fra，sys] 2016-04-11	该程序伪装成系统程序，安装无图标，运行后联网下载指定程序，执行静默安装操作，后续会根据网络获取的包名信息，静默卸载指定程序，存在一定的安全隐患，会给用户造成一定的资费消耗，建议及时卸载。（威胁等级低）
		Trojan/Android.lifering.a[prv，rmt] 2016-04-12	该程序运行获取短信指令，窃取用户地理位置信息，发送反馈短信，加载启动指定组件，存在一定的安全风险，会造成用户隐私泄露，建议及时卸载。（威胁等级中）
		Trojan/Android.Fakexlight.a[exp，rmt，sys]2016-04-13	该程序运行后联网下载恶意子包，尝试获取 root 权限，静默安装子包至系统目录，含有监听网络远程指令的功能，会执行下载、安装、卸载指定程序等敏感操作，存在发送恶意扣费行为代码，会给用户造成一定的安全隐患和资费消耗，建议及时卸载。（威胁等级高）
		Trojan/Android.poemsion.d[sys，exp] 2016-04-14	该程序是一个插件，运行后下载恶意 apk 并私自提权移动到系统目录下静默安装，建议立即卸载。（威胁等级中）
		RiskWare/Android.E4AQQspy.d[prv] 2016-04-15	该程序为一款卡 qq 在线程序，e4a 语言编写，使用过程中要求输入账号密码，可能会泄露 QQ 账号信息，为了 QQ 账号信息的安全，建议不要使用该软件。（威胁等级中）
	较为活跃的样本	Trojan/Android.Triada.e[prv，exp]	该程序包含非正规支付插件，运行会拦截指定短信执行屏蔽操作，上传用户来信内容，会造成隐私泄露，建议及时卸载。（威胁等级中）
		Trojan/Android.gaojipay.b[pay，sys]	该程序运行后会隐藏图标，释放资源文件下恶意子包文件，执行联网获取付费数据，后台发送扣费短信操作，给用户造成经济损失，建议及时卸载。（威胁等级中）
		Trojan/Android.SmsThief.ag[prv]	该应用假冒建设银行，运行后闪退并隐藏图标，后台监听指定短信上传到 http 服务器，窃取用户隐私，建议立即卸载。（威胁等级中）
		Tool/Android.GPSSpy.g[prv，spy]	该应用为一款定位查找工具软件，通过设置某个手机号码为信任号码，当收到该号码发送的带有 rqn 字符的短信时，会回复位置信息和电量给该号码；若设置了上传功能，则会定时将位置和电量信息上传到服务器。该应用会泄露位置信息，若非主动安装，建议谨慎使用。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 无效索引远程执行代码漏洞 (CVE-2014-6334)	如果 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，则会导致当前用户的上下文中存在远程执行代码漏洞。这可能允许攻击者执行任意代码，从而损坏系统内存。以下产品会受到影响：Microsoft Word 2007 SP3，Word Viewer，Office Compatibility Pack SP3。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/JS.Agent	此威胁是一个具有下载行为的 JS 木马程序，通常是嵌入到网页中，当用户访问带有木马链接的页面时，则会通过 JS 木马进行下载其他恶意程序。（威胁等级中）
		Trojan[Dropper]/VBS.Agent	此威胁是一种具有捆绑行为的木马程序，该家族会携带各种恶意软件，运行后会释放恶意软件并运行，窃取用户信息，占用系统资源，影响用户使用。（威胁等级中）
		GrayWare[AdWare]/Win32.Linkury	此威胁是一种有广告行为的木马类程序，会在未经同意的情况下，下载并安装多个程序，如：IE 搜索条，推广的软件程序等。（威胁等级低）

参议院推出立法　禁止端对端加密

Jenna McLaughlin/ 文　安天公益翻译小组 / 译

由参议院情报委员会领导人编写的反加密立法草案于近日发布，众多批评者对此愤怒不已。

该法案由参议员理查德·伯尔和黛安娜·范斯坦提交，它迫使技术公司要么为执法机构解密其客户的通信内容，要么黑进自己的产品以获取客户的通信内容，从而有效地禁止目前一些最重要的产品提供的端对端加密，包括 Apple、Facebook、Google 和 WhatsApp。

范斯坦和伯尔告诉记者，他们还在研究该草案，你无法对一个未完成的版本发表评论。

去年 12 月，范斯坦就下了战书，发誓要推出一项法案，强制科技公司采用可破解的加密方法。预期了最坏情况的隐私倡导者们对此并不感到吃惊。

参议员罗恩·维登 (民主党，俄勒冈州) 在发送给 The Intercept 的一份电子邮件称：“该立法规定，公司可以将后门设计成自己希望的样子，但肯定会要求他们建立后门。这在美国是第一次，那些想要为客户提供更高安全性的公司将需要决定如何削弱他们自己的产品，使用户更加不安全，而且他们毫无选择余地。”

“伯尔 – 范斯坦法案可能是我见过最荒唐的立法。这是用法律术语‘变魔术’呢。”卡托研究所的高级隐私和技术研究员朱利安·桑切斯在推特中说。

约翰·霍普金斯大学加密学教授马修·格林在推特中说：“若我所料，伯尔 – 范斯坦法案将是毫无依据的，也是行不通的。”

技术专家认为，无法设计一种能够被执法机构轻易破解，同时又能保护客户通信不被犯罪分子和黑客获取的强大加密功能。

该草案的开篇指出：“任何人或实体都不能凌驾于法律之上。通信服务和产品 (包括软件) 的所有供应商都应采用适当的数据安全方法来保护美籍人士的隐私，但是他们同时还应尊重法律，遵守所有法律要求和法院命令。”

该法案明确要求企业“及时”解密通信或提供“技术援助”，以破解任何安全措施并获得“可理解的”数据。这正是 FBI(美国联邦调查局) 命令苹果做的事情，目的是解锁圣贝纳迪诺枪击事件凶犯赛义德·里兹万·法鲁克 (Syed Rizwan Farook) 的工作手机。

苹果据理力争，指出，要想破解该手机的安全功能，公司需要设计一种软件“毒瘤”，这会威胁所有苹果用户的安全。

在这种情况下，FBI 援引《所有令状法案》作为依据，迫使苹果提供“合理的援助”，根据授权令解锁手机。该草案则更近了一步。专门从事计算机犯罪研究的乔治华盛顿大学法学教授奥林·克尔在推特中指出：“伯尔 – 范斯坦法案不只要求合理援助，还要求‘必要的援助’来解密设备。”

所有通信“产品”的供应商，包括几乎所有的智能手机供应商，也要对提供加密服务的第三方应用程序负责。

在发送给 The Intercept 的邮件中，开放技术研究所主管凯文·班克斯顿指出：“该法案不仅破坏我们的安全，还是一个巨大的互联网审查法案，要求在线平台 (如 Apple App Store 和 Google Play Store) 实施管制，终止安全应用程序的传播。”计算机科学家乔纳森·梅耶分析了要求谷歌遵守该法案的危险，指出这与“现代化的软件平台完全不相容”。而对于不依赖于谷歌 Native Android 的应用程序来说，“这种立法障碍是不可逾越的”，他继续说。

该法案试图安抚公司，说他们不必重新设计自己的产品，“但是如果要遵守该法案，苹果就必须重新设计产品”，安全研究员和 iOS 专家乔纳森·扎德尔斯基在推特中指出。

原文名称	Bill That Would Ban End-to-End Encryption Savaged by Critics
作者简介	Jenna McLaughlin，一名记者和博客作者，研究监控和国家安全领域。
原文信息	2016 年 4 月 9 日《The Intercept》发布 原文地址 https://theintercept.com/2016/04/08/bill-that-would-ban-end-to-end-encryption-savaged-by-critics/
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《勒索软件 TeslaCrypt 再次来袭》报告

近日，安天追影小组发现了勒索软件 TeslaCrypt 的最新变种 TeslaCrypt 4.0，并开始进行跟踪分析。TeslaCrypt 是在 2015 年 2 月份左右被发现，其是在 Cryptolocker 的基础上修改而成的，在第一个版本中，TeslaCrypt 声称使用非对称 RSA-2048 加密算法，但实际上使用的是对称的 AES 加密算法，由此 Cisco（思科）发布了一款解密工具，在找到可恢复主密钥的 key.dat 文件时，可以解密被 TeslaCrypt 加密的文件；但在之后的多个版本中，TeslaCrypt 开始使用非对称的 RSA 加密算法，被加密的文件在无密钥的情况下已经无法成功被解密。

TeslaCrypt 4.0 在 2016 年 3 月份开始出现，使用的是 RSA-4096 加密算法，经追影小组分析，它具有多种特性，例如：加密文件后不修改原文件名、对抗安全工具、具有 PDB 路径、利用 CMD 自启动、使用非常规的函数调用、同一域名可以下载多个勒索软件等。同时，TeslaCrypt4.0 利用网站挂马和电子邮件进行传播，在国内网站挂马发现的较少，通常利用浏览器漏洞（Chrome、Firefox、Internet Explorer）、Flash 漏洞和 Adobe Reader 漏洞进行传播；而利用电子邮件传播的数量较多，安天追影小组发现的多起勒索软件事件也都是通过电子邮件传播的。

勒索软件的泛滥对企业和个人用户都具有极大的威胁，被加密后的文件无法恢复，将给用户造成巨大的损失。目前，安天智甲终端防护系统（IEP）可以在用户失误点击运行勒索软件时阻止其对用户文件进行加密，安天追影高级威胁分析系统（PTA）则具有自动识别未知勒索软件的能力。但解决勒索软件威胁问题除了安装安全产品、防护产品、备份产品外，更需要用户在接收邮件时谨慎小心，慎重打开邮件附件或点击邮件内的链接，尤其是来自陌生人的邮件。

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。

文件名	30CB7DB1371C01F930309CDB30FF429B
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	396 KB
MD5	30CB7DB1371C01F930309CDB30FF429B
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	动态行为

◆ 危险行为

行为描述	危险等级
删除自身	★★★★

该文件具有以下行为：删除自身、填充导入表（疑似壳）、读取自身文件、释放 PE 文件、设置调试器权限、获取系统内存、增加 run 自启动项、获取系统版本、打开自身进程文件、遍历进程、获取 socket 本地名称、复制自身文件、连接网络、创建特定窗体、获取驱动器类型、独占打开文件、获取计算机名称、获取主机用户名称、查找指定内核模块、隐藏文件、请求加载驱动的权限。

◆ 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）	★★	读取自身文件	★★
释放 PE 文件	★★	设置调试器权限	★
获取系统内存	★★	释放 PE 文件	★
获取系统版本	★★	增加 run 自启动项	★
遍历进程	★	打开自身进程文件	★
复制自身文件	★★	获取 socket 本地名称	★
创建特定窗体	★	连接网络	★
获取计算机名称	★	获取驱动器类型	★
查找指定内核模块	★	独占打开文件	★
请求加载驱动的权限	★	获取主机用户名称	★
隐藏文件	★★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=30CB7DB1371C01F930309CDB30FF429B