安天周观察

主办：安天　2016 年 5 月 23 日（总第 40 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天首席战略官方华当选网络安全产业联盟技术创新专业委员会主任

5 月 21 日，中国网络安全产业联盟“技术创新专业委员会”第一次筹备会议在北京召开，经全体参会人员投票选举，安天联合创始人，首席战略官方华当选为委员会主任，卫士通信息产业股份有限公司副总裁李新、北京神州绿盟信息安全科技股份有限公司高级副总裁叶晓虎、北京微步在线科技有限公司 CEO 薛峰、杭州海康威视技术股份有限公司网络安全实验室主任王滨当选为副主任。

安天专注威胁检测领域，重视技术创新，自 2000 年创立以来，下决心、有恒心、找重心，先后在骨干网络高速病毒检测引擎 (2002)、大规模恶意代码的自动化分析处理 (2005)、先进移动病毒检测引擎 (2012) 等方面取得研发突破，也在高级威胁的检测与分析方面有一定进展和积累。安天的反病毒引擎技术在产业链中处于上游角色，全球有超过 30 家网络安全厂商、手机设备厂商和其他 IT 厂商选择安天引擎，来获得或提升检测能力。这些合作伙伴选择使用安天的反病毒引擎，可以减少反恶意代码方向的投入的人力，使自身将资源集中到更有价值的方向和功能上去，更深入的保障和达成用户价值。

方华，安天联合创始人，有超过 18 年的网络安全从业经验，一直担任安天首席战略官一职。

安天参加 2016 云计算大数据与安全峰会并发表主题演讲

5 月 19 日，由中国电子学会主办的 2016 云计算大数据与安全峰会在北京召开。本次峰会聚焦云计算大数据安全话题，邀请了云计算大数据安全专家、云安全提供方及云计算用户、白帽子现身说法，一起交流了云计算大数据安全的实践经验。

安天副总工、安全研究与应急处理中心（安天 CERT）负责人李柏松发表了题为《企业终端威胁预警云平台建设思路》的主题演讲，从近期安全研究人员捕获、分析和处理的安全事件出发，总结了当前重点行业网络和企业网络环境所面临的 APT 攻击、勒索软件等典型终端安全威胁，对关键基础设施防范的关键问题，如预防、检测、防护、响应等方面提出了建议，并通过动画演示，与大家一起探讨了基于 SaaS 模式的针对终端威胁的预警云平台建设思路。李柏松还展示了安天针对终端威胁的预警云平台建设思路提出的未知防御、全网追溯、定点清除的过程。首先针对不同企业使用的黑白名单，形成单独的安全基线，保证网络设备的安全运行；其次，进行深度威胁鉴定，通过前置沙箱发现未知漏洞和可疑行为；三，进行全网追溯，一旦发生事件，可在内网进行追溯；四，定点清除，由管理员进行清除；最后，面向勒索软件提出文档跟踪备份，利用云存储的优势，通过终端程序来跟踪文档的变化。

李柏松指出，攻击者和防御者之间是道高一尺魔高一丈的攻防博弈过程。在云计算方面，安天依托于多年的技术积累与前沿探索，结合对于行业的理解，针对云防御特点，提供了适合云使用的无代理模式和轻代理模式的反病毒引擎，使云端数据能够获得保障，目前已经与合作伙伴和业内友商进行了联合推广。

会议预告

2016 中国网络安全年会即将举行

由国家计算机网络应急技术处理协调中心主办的“2016 中国网络安全年会”将于 5 月 24 日至 26 日，在四川成都举行。届时，安天联合创始人，首席战略官方华将于 5 月 25 日，在大会主会场发表题为《熊猫的伤痕——几例中国遭遇 APT 攻击的案例分析》的技术演讲。安天移动安全公司总经理潘宣辰将于 5 月 26 日，在“移动互联网安全生态”分论坛发表题为《移动威胁情报体系支撑生态实践分享》的技术演讲。

赛门铁克核心杀毒引擎存在高危漏洞

近日，赛门铁克核心杀毒引擎被发现存在高危漏洞，该漏洞编号为 CVE-2016-2208，是一个远程代码执行漏洞，可通过向受害者发送包含文件的邮件或链接的方式加以利用。在 Linux、Mac 或 UNIX 平台上，会导致远程堆溢出；在 Windows 上，会导致内核内存损坏，因为杀毒软件的扫描引擎被加载到内核中，使得它变成一个远程的 ring0 内存损坏漏洞。（文章来源：http://sec.chinabyte.com/174/13782174.shtml）

每周安全事件

类 型	内 容
中文标题	至少 6 家国际银行遭到土耳其黑客团体攻击
英文标题	Six More Banks Supposedly Hacked by Turkish Hackers
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，土耳其黑客团体 Bozkurtlar（灰狼）对至少 6 家国际银行进行了网络攻击，成功窃取了部分数据。这 6 家银行包括：荷兰孟加拉银行（孟加拉共和国）、城市银行（孟加拉共和国）、信托银行（孟加拉共和国）、商业通用发展银行（尼泊尔）、Sanima Bank（尼泊尔）、锡兰商业银行（斯里兰卡）。泄露数据涉及客户数据、手机号码、加密密码等，此外还有大部分内部银行邮件通信文件，甚至还有服务器备份和银行金融声明等。
链接地址	http://news.softpedia.com/news/six-more-banks-supposedly-hacked-by-turkish-hackers-504069.shtml

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	G-Ware/Android.FAstroe.a[exp，rog]2016-05-16	该应用程序为非正规 App 市场程序，运行后会联网获取推送数据信息，后台频繁执行广告推送，影响用户正常体验，还含有风险代码，会执行私自下载操作，存在一定安全隐患，会造成用户资费消耗，建议及时卸载该程序。（威胁等级低）
		Trojan/Android.dxtDown.a[prv，rog]2016-05-17	该程序伪装成系统应用，安装无图标，开机自启动，运行后获取安装应用列表信息、浏览器书签、地理位置信息等上传到指定服务器，私自联网下载安装应用，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.atiSpy.a[prv]2016-05-17	该应用安装无图标，开机自启动，运行后获取用户手机号码、设备固件信息上传到远程服务器，还会监听短信，获取短信信息保存到数据库，并上传数据库内容到远程服务器，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.CxHanjica.a[prv，exp]2016-05-19	该程序运行后隐藏图标，后台获取用户通讯录和短信并通过邮件转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		G-Ware/Android.VikingHorde.a[prv，exp]2016-05-19	该应用包含恶意插件，运行后私自提权，调用关键 so 文件通过 socket 连接远程服务器，上传固件信息和 GPS 坐标，接受指令频繁联网，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级低）
		Trojan/Android.ContactSpy.a[prv]2016-05-20	该程序运行后会获取联系人、发件箱内容联网执行上传操作，会造成用户隐私泄露，建议及时卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.emial.dc[prv，exp]	该程序伪装成银联程序，运行隐藏图标，私发反馈信息，还会拦截短信，通过邮箱上传短信内容并执行屏蔽短信操作，造成用户隐私泄露，建议及时卸载。（威胁等级中）
		Trojan/Android.SmsSend.jn[prv，exp]	该程序伪装成系统程序，安装运行后隐藏图标，获取用户手机号码，在后台私自发送短信到指定号码，窃取用户隐私，建议立即卸载。（威胁等级中）
		Trojan/Android.Slocker.b[rmt，prv，rog，exp]	该应用伪装成系统短信应用，程序运行后会一直弹窗请求激活设备管理器，隐藏图标，后台联网上传用户设备相关信息以及短信信息，并获取指令执行拦截短信、发送短信、恢复出厂设置等行为，还会打开一个虚假的银行支付界面诱骗用户输入相关隐私信息并上传，造成用户隐私泄露和资费消耗。（威胁等级中）
		G-Ware/Android.Gluper.a[exp，rog]	该程序伪装成知名应用，安装无图标，后台联网下载 apk，可能用于推广广告，建议立即卸载，避免造成资费损耗。（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 故障索引远程内存破坏漏洞 (CVE-2014-6334)(MS14-069)	Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。Microsoft Word 2007 SP3，Word Viewer，Office Compatibility Pack SP3 版本在解析构造的 Office 文件时，没有正确处理内存对象，远程攻击者通过构造的 Office 文档，利用此漏洞可执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Drixed	此威胁是一种具有下载行为的木马类程序，样本运行后连接网络下载其他恶意代码并安装，占用系统资源。（威胁等级中）
		Trojan[Downloader]/MSWord.Steamilik	此威胁是一种具有下载行为的木马类程序，该家族通过垃圾邮件进行传播，样本为 Word 宏病毒，运行后连接网络下载其他恶意程序并运行。（威胁等级中）
		GrayWare[AdWare]/Win32.AdGazelle	此威胁是一种广告类程序，样本运行后是一款名为“HD Flash Player”的应用软件安装程序，点击同意后会连接网络下载并安装，占用系统资源，影响用户使用。（威胁等级中）

黑客论坛 Nulled.io 的 50 万用户信息遭泄

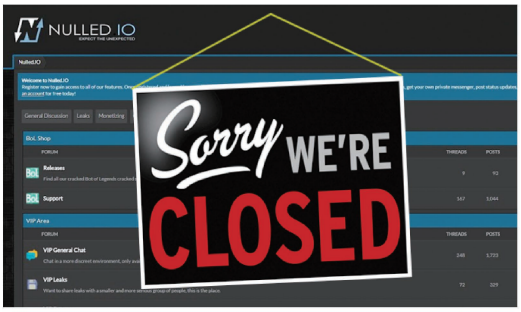
Chris Brook/ 文　安天公益翻译小组 / 译

近日，旨在帮助用户共享被盗凭证、软件漏洞和泄露信息的地下论坛 Nulled.io 遭到攻击，导致大量信息泄露，包括用户的电子邮件地址、加密密码和 IP 地址等。

随后，Risk Based Security 公司的安全研究人员发布了事件报告。报告显示，5 月 6 日，一个 1.30 GB 的 tar.gz 文件 (解压后是一个庞大的 9.45 GB SQL 文件) 被泄露。同时，留言板上的大量信息也被泄露，包括大约 536,064 名注册用户的详细信息和他们之间的 800,593 条个人消息。

该网站的口号是“期待意外之喜”，如今看来，颇具讽刺意味。目前，该网站已经下线。一则窗口消息称该服务正在进行“暂时的计划外维护”。

被泄露的信息包括：用户名、注册日期、注册 IP 地址和加密密码。一些用户的支付信息 (表格形式)，包括付款方式、贝宝电子邮件地址、日期和费用等也被泄露。其他潜在的个人身份信息 (包括 220 万帖子，其中很多是私人的，属于 VIP 专区)，3 个支付网关的 API 凭证和超过 90.7 万认证日志也被转储了。根据 Risk Based Security 的报告，我们可以将这些日志中的信息，包括地理位置数据、会员 ID、IP 地址和用户捐赠记录，拼凑起来，并与会员 ID 相匹配。同时，该公司表示，



能够追溯到捐赠记录的 5,582 条购买记录和 12,600 份账单也被转储了。

目前还不清楚该论坛是如何被攻击的，但是 Risk Based Security 指出，该网站运行着一个由 Invasion Power Services 创建的 IP.Board 论坛，而该论坛共有 185 个漏洞，其中的 92 个没有 CVE 命名。(Common Vulnerabilities and Exposures 通用漏洞披露，是国际上一个著名的漏洞数据库，为广泛认同的信息安全漏洞或者已经暴露出来的弱点给出一个公共的名称。使用一个共同的名字，可以帮助用户在各自独立的各种漏洞数据库中和漏洞评估工具中共享数据。)

Risk Based Security 公司发布博客称，最后一位用户登录论坛的时间是 5 月 6 日，这表明攻击可能发生在当日晚上。

网络安全公司 Sucuri 的首席技术官、创始人丹尼尔·西德在微博中警告说，这些论坛可能正合希望利用 ImageTragick 漏洞的攻击者的“心意”，他还补充说，他已经发现了针对 IP.Board 和 vBulletin 论坛的攻击企图。

本月初，我们概述了开源图像处理软件 ImageMagick 的漏洞。攻击者利用该漏洞，向该软件处理的图片中嵌入恶意代码，由此触发远程代码执行。

在梳理 Nulled.IO 数据库的时候，Risk Based Security 公司发现，365 名用户使用 .edu 地址访问该网站。其他 8 名用户通过 .gov 地址，以及约旦、巴西、马来西亚和土耳其的政府域电子邮件地址访问该网站。

当论及泄露的信息时，任何人 (包括执法机构) 都很可能轻易地将线索串起来。Risk Based Security 公司写到：“当诸如 Nulled.IO 的服务被攻击并导致数据泄露时，通常会暴露匿名用户的身份。简单地通过电子邮件或 IP 地址搜索，就会找到各种恶意行为的可能的幕后黑手。”

Risk Based Security 公司警告说：“有这么多的泄露数据，我们可以将会员 ID 与账单、交易和其他内容 (如会员消息和帖子) 相匹配。”

原文名称	Info on 500K Users Doxxed in Hacking Forum Dump
作者简介	Chris Brook，Threatpost 的副主编。
原文信息	2016 年 5 月 16 日《Threatpost》发布 原文地址 https://threatpost.com/info-on-500k-users-doxxed-in-hacking-forum-dump/118114/
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《又见 Locky 家族勒索软件》报告

近日，安天追影小组发现了一款传播热度上万的勒索软件，经分析后确认其为 Locky 勒索软件家族的新变种。此前，《安天周观察》曾在第 28 期发布《首例具有繁体中文提示的勒索软件 LOCKY》分析报告，指出这是一类利用垃圾邮件进行传播的勒索软件。

本次追影小组发现的样本可利用 word 文档中的宏代码下载勒索样本母体感染电脑，随后生成自身 ID，向 C2 服务器请求密钥，加密磁盘文件，用户硬盘中的文档、图片、视频、音乐等不同类型格式的文件都将被恶意控制。加密完成后，样本会根据用户电脑的语言环境来生成勒索提示语言。与其他 Locky 家族勒索软件一样，该样本的提示语言也是繁体中文。

根据提示信息可知，受害用户需要使用指定的“洋葱浏览器”(Tor Browser)，来交付赎金，并且需要以比特币为交易货币。而“洋葱浏览器”可以将用户的流量在世界各地的电脑终端跳跃式的传递，实现匿名访问，同时，比特币的交易更是难以追踪。

一个看似无害的 Word 文档都可以具有如此大的杀伤力，是由于大部分用户经常使用 Word，对这种文档缺乏防备之心，而黑客正是利用了这一心理漏洞来进行犯罪的。安天提醒广大用户，不要下载不明来源的附件，也不要随意打开链接，很多恶意软件都是通过网页挂马或钓鱼电子邮件的附件形式传播的。

养成良好的上网习惯，既可以避免大部分恶意软件的侵害，也可以缩小黑客的生存空间。安天追影小组将持续关注与分析勒索软件的传播态势，为用户提出更多合理的建议。

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、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。

最终依据静态分析鉴定器、动态行为鉴定器、智能学习鉴定器将文件判定为木马程序。

该文件具有以下行为：

格式漏洞、可疑进程名称、隐藏文件、获取系统内存、获取系统版本、获取计算机名称、获取 socket 本地名称、连接网络、创建特定窗体、获取驱动器类型、独占打开文件、打开自身进程文件、获取主机用户名称、查找特定窗体、请求加载驱动的权限。

文件名	C67C6394BFDB1CAD063383781C0476B6
文件类型	Document/Microsoft.DOC[:Word 98-2003]
大小	37 KB
MD5	C67C6394BFDB1CAD063383781C0476B6
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Downloader]/VBS.Agent.bpe
判定依据	静态分析

◆ 危险行为

行为描述	危险等级
格式漏洞	★★★★
可疑进程名称	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
隐藏文件	★	获取系统内存	★★
获取计算机名称	★	获取系统版本	★★
连接网络	★	获取 socket 本地名称	★
获取驱动器类型	★	创建特定窗体	★
打开自身进程文件	★	独占打开文件	★
查找特定窗体	★	获取主机用户名称	★
请求加载驱动的权限	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=C67C6394BFDB1CAD063383781C0476B6