安天周观察

主办：安天　2016 年 12 月 26 日（总第 70 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天荣获“2016 年度优秀技术支持单位”称号

2016 年 12 月 21 日，国家计算机病毒应急处理中心在天津召开“2016 信息安全企业座谈会”。会议授予安天、奇虎 360、卡巴斯基、腾讯、瑞星等十家企业“2016 年度优秀技术支持单位”称号。

天津市公安局网安总队总队长、国家计算机病毒应急处理中心主任张建成和公安部网络安全保卫局七处副处长祝国邦出席会议，并与参会企业代表进行了座谈交流。安天负责人向大会做工作报告。

安天负责人详细介绍了安天近期工作内容及取得成果，并表示安天将一如既往的委派专人负责与中心对接，从技术和管理等各个层次，全方位、全天候的响应中心的各项需要，为中心的案例侦破、态势监测、疫情监控等提供全方位的、力所能及的支援和支持。

近年来，安天多次在重大网络事故和网络安全事件的响应中发挥关键作用，参加了十七大、十八大、2010 年起的历届两会、北京奥运会等重大活动的网络安保工作，并荣获重大活动信息安全保卫工作突出贡献奖。同时，安天为用户和公众提供重大恶意代码和安全事件的应急响应服务。

在历史上，安天率先发现了红色代码 II、口令蠕虫等恶意代码，并在冲击波、魔波、震荡波、震网等恶意代码和重大安全攻击事件中，为国家有关部门和公众提供了有力的技术支持，发布了深度分析报告和有效应对方案。

安天参加 2016 年网络安全湖南峰会

2016 年 12 月 23 日，2016 年网络安全湖南峰会在长沙举行。来自网信、经信、公安、国安、新闻出版、通信管理、保密、密码管理、国防动员等系统的 1200 余名代表参会，共谋互联网安全之道。安天技术负责人应邀在大会作了《从呈现对手的视角看态势感知》的报告，他从安天团队持续捕获的多起 APT 事件入手，并以可视化的方式复盘了相关事件，从“阻塞、呈现和切断”对手的攻击链的思路分享了防御分析经验。并介绍了安天在“全域感知、融合防御”方面做的一些探索。

■ 安天收到北京航天飞行控制中心感谢信

2016 年 12 月 20 日，北京航天飞行控制中心向安天发来感谢信，感谢安天在天宫二号与神舟十一号载人飞行任务中所作出的贡献。

天宫二号与神舟十一号载人飞行任务任务是我国空间实验室建设的关键之战、奠基之战。安天在任务的准备和实施工作过程中为网络和系统提供安保服务。北京航天飞行控制中心对安天的工作表示认可，并对安天在安保中提供的“智甲”终端防御系统（即私有云安全防护系统）和“探海”威胁检测系统给予了赞赏，认为其在任务中运行稳定可靠，为任务的圆满成功做出了重要贡献。

近年来，安天多次在重大网络事故和网络安全事件的响应中发挥关键作用。安天探海、追影、智甲等产品为很多关键客户提供了安全保障，多次收到来自用户和主管部门的肯定。

■ 安天荣获“2016 龙江企业社会责任开拓创新奖”

2016 年 12 月 21 日，由黑龙江省精神文明办、黑龙江广播电视台共同举办的“龙江力量——2016 首届龙江企业社会责任榜”颁奖晚会圆满落幕。安天荣获“2016 龙江企业社会责任开拓创新奖”。

安天作为从哈尔滨起步的本土企业，一直坚持“扎根龙江、辐射全国、放眼世界”，凭借自身的技术实力、技术展现力和技术文化，逐渐成为黑龙江独有特色的高科技名片。2016 年 5 月 23 日至 25 日，习近平总书记在黑龙江考察调研期间，视察了安天总部，并听取了安天负责人对安天核心反病毒引擎技术、专利贮备、APT 高级威胁检测、防护产品和解决方案等的汇报。

■ 安天“追逐梦想”演唱会点燃冬日暖阳

2016 年 12 月 16 日，安天哈尔滨总部举办“追逐梦想”演唱会，来自安天多部门的员工激情开唱。由安天员工组建的傲气安天乐队为大家献上了十几首音乐，其中有由傲气安天乐队自己填词的安天主题曲《我们在路上》。

演唱会丰富了工程师紧张的工作，更传递了安天自由，民主，快乐的文化传统，现场气氛热烈，鼓舞斗志，点燃冬日温暖的希望，吹响新年奋进的号角。

每周安全事件

类 型	内 容
中文标题	全新 Alice ATM 恶意软件出现
英文标题	New Alice ATM Malware, a lightweight and efficient threat
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，安全专家们发现了一种新型的 ATM 恶意软件——Alice。Alice 的攻击机制旨在针对各类自助式服务 ATM 设备中的安全保护功能。此恶意软件非常值得关注，Alice 最大的特点就是它不同于其它 ATM 恶意软件。因为它无法实现数据窃取，亦不可通过 ATM 数字键盘进行控制，Alice 利用清空原有安全机制和实机操作取现。 研究人员最初于 2016 年 11 月发现 Alice 恶意软件，这项工作为 Trend Micro 与 Europol EC3 建立的联合研究项目的一部分，不过他们推测此恶意软件的诞生时间应该在 2014 年。在初次发现 Alice 时，研究人员们曾经怀疑其属于已知 ATM 恶意软件 Padpin 的新型变种。但经过进一步调查后，他们发现 Alice 属于一种全新恶意软件家族。
链接地址	http://securityaffairs.co/wordpress/54612/malware/alice-atm-malware.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 9 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.mobilenama.a[prv，spy]2016-12-20	该程序为间谍应用，运行后后台会窃取用户短信、通话记录、位置信息、通讯录等隐私信息并回传给攻击者，造成用户隐私泄露。建议卸载。（威胁等级高）
		Trojan/Android.SmsSend.lf[exp] 2016-12-21	该应用安装后无图标显示，开机后会自启动，运行后会私自发送短信并删除短信记录，拦截指定信息。为避免造成资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.E4AQQspy.q[prv] 2016-12-22	该软件会伪装成 QQ 插件工具，窃取用户的 QQ 账号密码，造成用户隐私泄露。建议立即卸载。（威胁等级高）
	较为活跃的样本	G-Ware/Android.konkoroid.a[rog，exp]	该应用运行后，后台会访问多个网址，并跳转到色情、广告、博彩等网站，同时会下载色情应用，造成用户资费损耗。建议卸载。（威胁等级中）
		Trojan/Android.Rootnik.o[rog，exp]	该应用是一款翻译工具，包含风险代码，运行后会释放恶意子包，私自提权，包含支付模块，存在拦截回复短信的行为。为避免造成资费损耗，建议立即卸载。（威胁等级高）
		G-Ware/Android.FakeSystem.d[exp，rog]	该应用伪装成系统应用，开机后会自启，访问指定 URL，造成用户流量耗费。建议立即卸载。（威胁等级中）
		G-Ware/Android.SysDown.a[rog，exp]	该应用伪装成系统程序，安装后无图标显示，后台会私自推送广告，连网下载推广应用，静默安装应用，建议卸载，避免造成资费损耗。（威胁等级低）
		Trojan/Android.Malapp.a[prv，exp]	该程序会接受短信远程控制，窃取用户 IMEI 码和位置信息，私自向指定号码发送短信。为避免造成资费损耗和隐私泄露，建议卸载。（威胁等级中）
		G-Ware/Android.LKCF.a[rog，exp]	该应用伪装成系统应用，会捆绑广告插件，运行后会隐藏图标，在手机屏幕匿名弹窗，强行推送广告，上传用户手机固件信息。严重干扰手机的正常使用，造成用户流量资费损耗。建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 文件堆溢出 CVE-2014-6334 内存破坏漏洞 (MS16-004)	Microsoft Office 未能正确解析 RTF 文档所造成的堆溢出漏洞，攻击者可以利用此漏洞执行远程代码。其根本原因是控制拷贝至堆缓冲区的长度从而造成堆溢出。以下产品受到影响：Microsoft Office 2007 SP3、2010 SP2、2013 SP1、2013 RT SP1、2016、Excel 2016 for Mac、PowerPoint 2016 for Mac、Word 2016 for Mac 和 Word Viewer。（威胁等级高）
	较为活跃的样本	Trojan[Exploit]/SWF.Angler	此威胁是一类可以利用软件漏洞的木马家族，该家族因 Angler Exploit Kit 而得名，此家族样本使用了 SWF 漏洞对用户的设备进行感染，从而执行任意恶意代码。（威胁等级高）
		Trojan/BAT.LockRar	此威胁是一种可以加密用户文件的木马家族，该家族样本以 BAT 批处理脚本形式存在。此家族样本执行后会对系统中的文件进行加密。（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家族的统称，该家族样本在执行后会利用 Shell Execute 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/Multi.Remsec	此威胁是一种可以窃取用户敏感信息的木马家族，该家族是一种远程控制的后门程序，在多个平台上都具有效力，在执行后攻击者会获得计算机的全部权限。（威胁等级高）

多达 10 亿雅虎账户被盗

Lily Hay Newman / 文　安天公益翻译小组 / 译

2016 年 9 月，雅虎因宣布 5 亿用户账户信息泄露而受到广泛关注。近期，雅虎再次宣布，在 2013 年 8 月的一次攻击中，黑客窃取了雅虎 10 亿用户的账户。

攻击简介

目前，我们所知道的最重要的信息是：此次泄露事件很可能不同于雅虎在 2016 年 9 月 22 日披露的事件。后者发生在 2014 年底，而前者则更早一年。雅虎一直在与执法部门和第三方网络安全公司合作，以验证攻击事件并追溯其起源。但是雅虎指出，到目前为止，还未知晓攻击者的身份。

雅虎表示，泄露的数据包括用户的姓名、电子邮件地址、电话号码、生日、哈希加密的密码，以及加密和未加密的安全问题和答案。雅虎表示被盗的数据不包括未加密的密码、信用卡号码或银行账户信息。具体来说，金融数据存储在一个单独的系统中，雅虎相信该系统未被入侵。

2015 年和 2016 年，雅虎也发生了数据泄露事件。黑客使用伪造的 Cookie 绕过安全保护，并在没有密码的情况下访问用户的账户。雅虎认为，该攻击与某些国家赞助的黑客有些关系，2014 年的数据泄露事件也是这些黑客的杰作。

21 世纪初曾担任两年雅虎信息安全官的杰里米亚·格罗斯曼（Jeremiah Grossman）指出：“如果在两三年前，这种事情可能发生在任何人身上，每个人都可能发生重大的数据泄露事件。但是，雅虎数据泄露事件的细节表明，该公司的数据管理存在混乱，安全团队没有获得足够的支持。”

谁受到了影响?

该攻击感染的账户可能与今年 9 月公布感染账户存在重叠。但是即使是在最好的情况下，也至少有 10 亿雅虎账户被黑了，而更坏的情况则是有 15 亿账户被黑了。因为，2013 年秋季，雅虎宣布它的月活跃用户有 8 亿，但尚不清楚它到底有多少不活跃的用户。无论怎样，如果你在 2013 年或 2014 年注册了雅虎账户，你都需要立即重置密码和安全问题。不幸的是，数据泄露造成的损害将无法完全消除。“鉴于此次数据泄露发生在三年前，我想知道在过去的三年中有多少泄露事件源于从雅虎窃取的数据。”格罗斯曼说。

有多严重?

考虑到数据泄露大约涉及到 30 亿互联网用户，其中包括 10 亿活跃用户，因此雅虎花了这么长的时间才发现数据泄露。在过去，许多机构没有投入足够的资源来保护他们的网络和数字基础设施。一方面是他们认为不需要，所以不会将此优先考虑在预算中，另一方面则是他们认为黑客攻击不会发生在他们身上。雅虎似乎犯了其中的一个错误或上述所有错误。

虽然密码采用哈希加密，但是该方法存着漏洞，这就意味着用户的账户并不安全。雅虎表示，他们正在通知受此次数据泄露事件影响的用户，并要求所有用户更改密码，还取消了加密的安全问题。

此次数据泄露不光严重影响了雅虎的用户，也可能影响威瑞信对雅虎核心互联网业务的收购。《纽约邮报》曾报道，今年 9 月雅虎曝出数据泄露之后，威瑞信要求雅虎将 48 亿美元的交易减少 10 亿美元。威瑞信尚未回应近期曝出的黑客攻击事件。

希望这是雅虎需要处理的最后一次泄露事件，但是雅虎将难以挽回消费者和企业的信任，因为这些泄露事件的影响还未全部体现出来。格罗斯曼说：“我们怎么能肯定雅虎真的赶跑了黑客？毕竟黑客有三年的时间隐藏在系统中。我认为，如果雅虎将任务透明化，我们则是可以确定它真的赶跑了黑客的，但是让雅虎任务透明化却很难做到的。”

原文名称	Hackers Breach a Billion Yahoo Accounts
作者简介	Lily Hay Newman，《连线杂志》安全领域作者。
原文信息	2016 年 12 月 14 日发布于《连线杂志》，原文地址 https://www.wired.com/2016/12/yahoo-hack-billion-users/
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《窃取 POS 系统数据的恶意软件 FlokiBot 介绍》

近日，安天追影小组在进行日常安全事件梳理时，关注到一个基于 Zeus 木马家族相同代码库的新型银行恶意软件变种——FlokiBot 家族，其最近已经在各种黑客市场上销售，FlokiBot 不仅复制了 Zeus 家族中存在的功能特征，还增加了新功能，使其成为一个有吸引力的工具。攻击者可利用 RIG 工具进行鱼叉式钓鱼攻击 POS 系统进行数据窃取。

FlokiBot 恶意软件起源于病毒家族 Zeus2.0.8.9 源码，并存在多个变种，其同时支持英语、俄语、葡萄牙语等多种语言，主要目标是窃取 POS 刷卡机数据。一旦 FlokiBot 恶意软件执行，其先会尝试注入“explorer.exe”进程，如果失败，则会注入到“svchost.exe”进程。该恶意软件会根据执行环境，注入不同的资源数据，包括“key”、“bot32”、“bot64”。注入的资源数据使用了 RC4 加密，并使用 LZNT1 算法压缩。

另外，此恶意软件使用散列算法，来模糊动态库解析中使用的模块和函数名称，以此防止杀毒软件的查杀。若其注入成功，杀毒软件会监控到进程“explorer.exe”或“svchost.exe”使用 HTTPS 协议与 C2 进行通信。

在其网络通信行为中，FlokiBot 沿用了 Zeus 家族的一个防深度包检测功能，网络数据包中的字节被封装在通过 HTTPS 发送的 BinStorage 结构中并进行多层加密。其首包解密后的内容是有关受感染机器的信息，如计算机名称和屏幕分辨率。

另外，对其网络相关配置进行分析后，发现其对 localhost 的 9050 端口进行监控，这是一个标准 Tor 代理服务器监听配置设置方式，猜测其也支持 Tor 网络。

随着使用 POS 机刷卡消费的普遍，对应的 POS 系统中会存储大量的用户信息，这关系到用户的切身财产安全，也为攻击者谋取利益提供了空间。安天提醒相关使用 POS 系统的企业单位以及使用 POS 机刷卡的用户，关注 POS 卡的使用安全。

为对此类威胁做及时响应处理，安天将长期关注 FlokiBot 家族的变化及收集并分析该家族相关样本，以深入了解此恶意软件变种，以确定 FlokiBot 的技术能力和特性，为用户提出更合理的建议。

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，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：

请求加载驱动的权限、创建特定窗体、获取驱动器类型、获取系统内存、独占打开文件、获取计算机名称、疑似查找浏览器进程。

文件名	5649E7A200DF2FB85AD1FB5A723BEF22
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	233 KB
MD5	5649E7A200DF2FB85AD1FB5A723BEF22
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Banker]/Win32.FlokiBot.Pos
判定依据	动态行为

报告地址：https://antiy.pta.center/_lk/details.html?hash=5649E7A200DF2FB85AD1FB5A723BEF22

◆ 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
请求加载驱动的权限	★★	创建特定窗体	★
获取驱动器类型	★	获取系统内存	★★
独占打开文件	★	获取计算机名称	★
疑似查找浏览器进程	★★		