安天周观察

主办：安天　2016 年 6 月 20 日（总第 44 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参展第四届新博会和第二十七届哈洽会

6 月 15 日至 19 日，第四届中国国际新材料产业博览会和第二十七届哈尔滨国际经济贸易洽谈会在哈尔滨国际会展体育中心同期举行。在本届展会中，网信专题被第一次纳入到整体活动当中，大会首次设立了“网络空间及互联网 +”展区，并下设“网络安全板块”。作为将基础能力扎根于哈尔滨的网络安全企业，安天成为了该板块的代表。

前不久，总书记在 4 月 19 日的网信座谈会讲话中提出了做好“全天候全方位态势感知工作”的工作要求，要求网安工作者解决“谁进来了不知道、是敌是友不知道、干了什么不知道”的问题。在展会现场，安天通过“监控预警平台及可视化展示系统”动态地展示了监控预警平台的部署和全球恶意代码的安全态势，使现场观众对全球恶意威胁的态势有了直观的认识。

“安天监控预警平台及可视化展示系统”是基于安天产品：“追影”威胁分析系统 (PTA)、“探海”威胁检测系统 (PTD)、“镇关”威胁阻断系统 (PTF)、“智甲”终端威胁防护系统 (IEP) 等建立的适应性强且技术能力国内领先的网络犯罪感知发现、深度分析、追踪溯源的恶意代码和高级威胁检测能力部署，通过安天安全可视化管理平台进行统一管理，通过该平台，用户可以对网络侧、终端侧的威胁事件进行密切监控，实时跟踪可疑文件信息并进行多维度的数据挖掘，从而达到掌握安全态势，发现高级威胁的目的。目前，安天的各款产品在海关总署、某国防院校安全防护平台、某市公安局公共信息网络安全综合管理系统等网络安全出口均有部署。

同时，安天遵循“原创、沉淀、分享”的原则，在展会现场免费发送了安天 2015 年度的传统威胁年报、移动威胁年报以及安天技术文章汇编《高级持续性威胁 (APT) 专题 · 第二分册》和《工控系统安全分册》等资料，分享了自己的分析成果和研究进展，受到了安全爱好者的好评。

北约正式将『网络』确定为战场

近日，北大西洋公约组织秘书长斯托尔滕贝格在比利时布鲁塞尔的一场新闻发布会上宣布，“网络”将正式成为各北约成员国的战场。

这也意味着对北约成员国中任何一国的网络攻击将被视为对整个联盟的攻击，所有成员国应援助受攻击国家。目前，大多数北约成员国已经确定将网络作为一个正式的战场，并在他们的军队建立了网络安全部门。比如美国海军陆战队和美国海军今年就宣布将成立全新的网络安全部门，开展网络空间防御行动。（文章来源：http://news.softpedia.com/news/nato-declares-cyber-as-official-battleground-next-to-air-sea-and-land-505388.shtml）

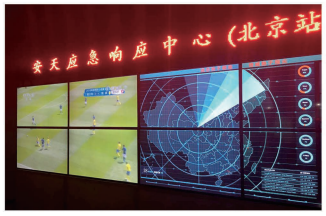
一周简讯

- 社工手段达到新水平，攻击者冒用谷歌身份绕过谷歌双因素验证
- 韩国称朝鲜向其 14 万台电脑植入恶意代码，计划发动大规模网络攻击
- 美国 NSA 及情报机构：不排除通过入侵物联网医疗设备收集情报
- 安全厂商发现俄罗斯 APT28 组织对美国政府机构发起钓鱼攻击
- 微软 OLE 技术被滥用，将恶意代码嵌入 Office 文档，类似宏病毒
- 安天发布远程控制木马预警：假借知名应用植入恶意模块
- 研究人员发现银行木马 Vawtrack v2 活跃，目标范围扩大至更多国家

（安天 CERT 搜集整理，详见：http://bbs.antiy.cn）

安天北京公司实况转播欧洲杯

6 月 17 日，安天北京公司实况转播了欧洲杯小组赛意大利对战瑞典的比赛。在一周忙碌的工作之余，能用“超大屏”享受一场激情四射的足球比赛，安天北京小伙伴的这个周五真是劳逸结合的典范。



每周安全事件

类 型	内 容
中文标题	南非广播公司遭受匿名黑客 DDoS 攻击
英文标题	Anonymous hacktivists hit South African state broadcaster over censorship
作者及单位	Jason Murdock；IB Times
内容概述	近日，南非最大的官方国家广播公司——南非广播公司 (SABC) 遭到了黑客组织 Anonymous Africa 的匿名攻击。黑客对 SABC 主要电视频道和广播电台的网站实施了 DDoS 攻击。黑客在攻陷了所有网络相关服务后，又延续了四个小时的攻击。SABC 发言人 Kazier Kganyago 证实了此次攻击，并称 SABC 将对此展开调查，找出罪魁祸首。
链接地址	http://www.ibtimes.co.uk/anonymous-hacktivists-hit-south-african-state-broadcaster-over-censorship-1565202

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.turtle.a[rmt, prv, spy]2016-06-13	该应用是间谍软件，通过接收指令完成锁屏、打开浏览器、隐藏图标、发送短信、锁定界面等功能，同时获取用户的收件箱内容、联系人、手机 IP 地址、手机版本信息和通话录音并上传到指定服务器，会造成隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		G-Ware/Android.FtpadAd.a[rog, exp] 2016-06-13	该应用伪装成系统程序，安装无图标，运行后诱导激活设备管理器，联网获取推广数据，执行创建桌面图标推广操作，还包含风险代码，尝试提权静默安装未知子包，存在一定安全风险，会造成用户资费消耗，建议及时卸载。（威胁等级低）
		Trojan/Android.Hqwar.a[prv, exp, rmt, sys] 2016-06-15	该应用伪装成知名游戏应用，运行后隐藏图标，诱导激活设备管理器，接收短信指令，上传通讯录和信箱等隐私信息，进行发送短信、回复短信、拨打电话、卸载指定 apk、联网下载 apk 并弹出诱导安装等操作。建议立即卸载，避免造成隐私泄露和资费损耗。（威胁等级高）
		Trojan/Android.privacySteal.a[prv, exp, rmt] 2016-06-15	该应用伪装成系统程序，运行后诱导激活设备管理器，隐藏桌面图标，监听手机通话，开启通话录音，上传通讯录和录音文件，监听短信指令，执行发送指定短信、设置屏蔽指定短信、开启环境录音、上传短信箱内容等操作，会造成用户隐私泄露，建议及时卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.banksteal.c[prv, exp, rmt, sys]	该程序伪装成知名应用，运行后诱导激活设备管理器并隐藏图标，后台窃取用户银行账户密码上传到远程服务器，接收指令上传用户信箱、安装列表、通话记录、通讯录等隐私信息，执行拨打电话、发送短信、删除短信等操作，建议立即卸载，避免造成隐私泄露和资费损耗。（威胁等级高）
		G-Ware/Android.jianmo.ad[rog, exp]	该应用伪装成抢红包插件，运行后置顶界面，使手机无法正常使用，勒索用户添加指定 QQ 号码进行付费解锁，造成用户资费损耗，建议不要安装。（威胁等级低）
		G-Ware/Android.jianmo.ae[rog, exp]	该应用伪装成 QQ 刷钻工具，运行后激活设备管理器，使手机无法正常使用，勒索用户添加指定 QQ 号码进行付费，造成用户资费损耗，建议不要安装。（威胁等级低）
		G-Ware/Android.Downloader.bx[spr, exp]	该应用运行后会利用色情敏感内容诱骗用户下载安装恶意应用，造成用户资费消耗。（威胁等级低）
		Trojan/Android.Downloader.by[rog, exp]	该应用安装无图标，程序运行后会联网私自下载未知推送应用，并进行静默安装和启动，造成用户资费消耗。（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 未初始化内存使用漏洞 CVE-2015-1770	该漏洞可能在用户打开经特殊设计的 Microsoft Office 文件时允许远程执行代码。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Zurgop	此威胁是一种木马家族，运行后连接网络下载其他恶意代码并执行，可能会窃取用户敏感信息并回传，有一定的威胁。（威胁等级中）
		RiskWare[Downloader]/NSIS.YourInstaller	此威胁的家族样本运行后可以连接网络下载推广应用并安装，会占用系统资源，影响用户使用。（威胁等级中）
		Trojan[Ransom]/Win32.Cryptolocker	此威胁是一种勒索木马类程序，该家族样本使用 .NET 编写，使用记事本图标进行伪装，运行后会释放可执行文件到系统文件夹，遍历系统文件，对系统中文件进行加密操作。（威胁等级中）

ATM 恶意软件日益增加

David Sancho , Numaan Huq/ 文　安天公益翻译小组 / 译

随着时代的发展，自动取款机 (ATM) 已经不再仅受物理手段的影响了。现在，安全行业和执法机构认为，针对 ATM 的逻辑攻击是一种新威胁。近年来，众多研究人员发现了 ATM 恶意软件，也发现了它们被成功运用的事件。在这种类型的犯罪中，攻击者使用了专门针对 ATM 的恶意软件。攻击向数字化手段的转变表明，对于犯罪组织来说，使用恶意软件从 ATM 窃取资金和卡片信息更加容易，也更安全。未来，这种趋势会更加明显，我们应该关注犯罪组织创建的不同方法。

ATM 欺诈和物理攻击

根据统计数据表明，在过去的一年里，欧洲的 ATM 欺诈攻击普遍增加 (2014 年至 2015 年，ATM 欺诈攻击增加了 15%)。所有领域的软件攻击的增长趋势也意味着，最先进的犯罪组织已经意识到了黑客工具的隐藏机会。用于 ATM 欺诈的恶意软件虽然处于起步阶段，但是这一趋势是必然的。

虽然研究人员没有获得美国 ATM 恶意软件攻击的统计数据，但是欧洲 ATM 安全团队指出，“单一欧元支付区 (SEPA) 之外的 53 个国家和地区，以及之内的 10 个国家和地区都遭受了损失。据报道，损失最严重的前三个国家是美国、印度尼西亚和菲律宾。”

ATM 恶意软件是如何出现的?

目前，趋势科技和隶属于欧洲刑警组织的欧洲网络犯罪中心 (EC3) 展开了共同合作，研究针对 ATM 的不断变化的网络威胁。他们的研究表明，除了更为传统的攻击向量，还有很多因素促使黑客工具转向 ATM。

一个主要因素是使用过时的，已经不能再接收安全补丁的操作系统，如 Windows XP。另一个原因可能是犯罪分子日益成熟，他们意识到数字化方式风险较低，能够更为隐蔽地执行活动。还有一个重要因素是，ATM 厂商采用提供应用程序编程接口 (API) 的中间件与机器的外围设备 (如 PIN 键盘，自动提款机等) 通信。该中间件被称为金融服务扩展 (XFS) 中间件。简单来说，如果我们将现代化的 ATM 视为通过软件控制的、连接钞箱的 MS Windows 计算机，就能很容易地明白为什么它对恶意软件编写者充满了吸引力。

主要的 ATM 恶意软件家族

趋势科技和欧洲网络犯罪中心还合作研究了目前主要的恶意软件类型。研究表明，拉丁美洲和东欧的商业银行缺乏安全措施，为犯罪分子开启了攻击这些地区的 ATM 的大门。

图 1 中每个 ATM 恶意软件家族都具有特定的功能设置，可以通过两个主要特征加以区分：① ATM 制造商类型；②特定的恶意软件功能：读取用户输入的信息 (如卡号和密码)，或者吐出现金。这些恶意软件的共同点是，它们通常是通过 USB 或 CD 手动安装的。

图 1　ATM 恶意软件家族及其地理来源

研究还发现，除了拉丁美洲和东欧等高发区以外，ATM 恶意软件也慢慢地应用到了其他地区，虽然目前还没有看到地下市场交易 ATM 恶意软件，但是安全专家预计在不久的将来会出现这样的情况。

原文名称	ATM Malware on the Rise
作者简介	David Sancho、Numaan Huq，趋势科技的高级威胁研究员。
原文信息	2016 年 4 月 12 日趋势科技发布，原文地址 http://blog.trendmicro.com/trendlabs-security-intelligence/atm-malware-on-the-rise/
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《一款以 FTP 服务器为目标的蠕虫病毒分析报告》

近日，安天追影小组在持续追踪网络犯罪的过程中，发现了一种名为 PhotoMiner 的蠕虫病毒的新型变种。该变种具备独特的多级感染机制，样本图标是一个看似包含照片的文件夹，充分利用潜在受害者的隐私窥视心理，引诱其点击，属于典型的社会工程学手段。

在过去的几个月中，PhotoMiner 变种一直活跃于一些网站上。追影小组通过分析发现，这些网站所托管的 FTP 服务器大多是缺乏保护机制的，有的甚至是毫无保护的。攻击者可以利用弱账号密码字典进行暴力破解，获取 FTP 服务器登录账户密码，进而感染 FTP 服务器上托管的网站，将特定的恶意代码，如 PhotoMiner 变种等，传播到访问者的机器上。

一旦 PhotoMiner 变种成功感染受害者的机器，其就会大量消耗感染机器性能来进行门罗币挖矿，从而使攻击者获利。同时还会注册自身释放的恶意代码文件为系统启动项，以达到长期执行任务的目的。另外，PhotoMiner 还具备内网传播感染的能力，其使用内置的 Windows 系统工具，如“ATP”和“NET VIEW”等读取 ARP 缓存，扫描使用浏览器协议的本地网段，进而尝试暴力连接本地网段内地址，一旦连接成功，就将自身复制到一个可以进行可访问的启动位置，从而感染更多的 FTP 服务器和用户系统。

经过以上分析，安天追影小组认为，这种通过攻击缺乏保护的 FTP 服务器来感染网站的传统攻击方式，在近期也许会再次流行。为了避免成为僵尸网络的受害者，安天追影小组提醒广大用户加强网络安全意识，不要随意打开陌生链接，也不要随意运行不明应用程序，同时要及时地更新杀毒软件。

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，即可实现对上述高级威胁进行有效检测，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 BD 静态分析鉴定器、静态分析鉴定器、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：疑似已知恶意软件变种、自启动、连接网络、获取 socket 本地名称。

文件名	ABA2D86ED17F587EB6D57E6C75F64F05
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.51 MB
MD5	ABA2D86ED17F587EB6D57E6C75F64F05
病毒类型	高级威胁
恶意判定 / 病毒名称	Trojan[PSW]/Win32.Tepfer
判定依据	静态分析

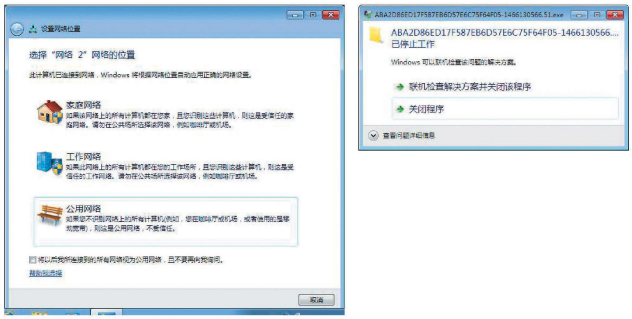
◆ 危险行为

行为描述	危险等级	行为描述	危险等级
疑似已知恶意软件变种	★★★★★	自启动	★★★★★

◆ 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 socket 本地名称	★

◆ 动态截屏



◆ 静态启发式检测

检测类型	检测点	详细说明
PE 结构	含有 tls 表	恶意代码作者常用的反调试技术。PE 结构中的 TLS 结构早于程序运行。
编译指令	未知壳	未被公开的壳，经常被恶意代码使用，用来保护恶意程序被查杀。
PE 结构	无版本信息并且不是 GCC 编译器	除 GCC 编译器外，常规编译器均默认包含版本信息。如果不是 GCC 编译器，并且不包含版本信息，显然是作者故意抹掉版本信息，逃避追查。

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=ABA2D86ED17F587EB6D57E6C75F64F05