安天周观察

主办：安天　2016 年 6 月 27 日（总第 45 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天再获“中国互联网行业自律贡献奖”

6 月 23 日，在“2016 年中国互联网大会”闭幕论坛上，中国互联网协会为 360 公司、阿里巴巴、爱奇艺、安天等 30 家单位颁发了 2014-2016 年度“中国互联网行业自律贡献奖”。这是继 2012-2014 年度以来，安天第二次获得该殊荣，安天也因此成为了连续两次荣获该奖项的专业网络安全厂商。

“中国互联网行业自律贡献奖”在 2014 年首次设立，旨在加强我国互联网行业的自律意识，表彰在实施互联网自律中做出突出贡献的从业单位或个人。具有引导互联网企业认真履行社会责任，树立良好社会形象，推动互联网行业健康发展的重要作用。

“安全”是互联网行业中一个特殊的领域，安全企业不仅需要有良好的职业道德，更需要从维护国家和行业整体利益的高度出发，推动行业自律，创造良好的行业发展环境。

作为一个网络安全厂商，安天严格遵守《中国互联网行业自律公约》，始终站在应对威胁的第一线，致力于提供先进的威胁检测能力，为超过 6 万台防火墙、UTM 等安全设备和近 2 亿部手机终端中的安全产品提供安全保障；为公众提供重大恶意代码和安全事件的应急响应服务；积极参与行业建设，倡导合法、公平、有序的行业竞争；乐于分享研究成果，发表了大量的分析报告和技术文献；重视知识产权保护工作，申请专利 407 项，取得授权 115 项。

安天以恪守传统反病毒价值观为原则，坚持防御者的立场，坚持保障用户价值的使命，坚持对安全威胁受害者感同身受的情感，坚持对原则和底线的敬畏。为“服务客户，解决问题。应对威胁，保障价值！”做出不懈努力。

一周简讯

- 报告显示，83% 受测企业网络的 DNS 存在恶意活动迹象
- 比特币采矿恶意代码活动借助社会工程手段死灰复燃
- 钓鱼攻击新伎俩：从网址托管公司租用临时 URL 地址
- Uber 网站和服务器存在漏洞，可泄露乘客个人信息
- 工信部将建国家级网络安全信息共享数据库
- 世界最大僵尸网络 Necurs 的 C&C 再度活跃
- 开源压缩工具包 Libarchive 出现安全漏洞，几百个项目受影响

（安天 CERT 搜集整理，详见：http://bbs.antiy.cn）

安天亮相 NSC2016 中国网络安全大会

6 月 23 日，第四届中国网络安全大会在国家会议中心召开，安天携移动威胁情报平台 AVL Insight 和反 APT 综合解决方案参加了本次会议。

作为国内首个移动威胁情报平台，AVL Insight 可通过对移动威胁的全面感知和快速分析响应，多维度呈现高价值、定制化情报信息，并提供移动威胁的预警和处置策略。该平台旨在提高银行、政府等大型机构对威胁事件的感知、预警、预防、取证、响应和处置能力，以达到降低 IT 安全成本，提高资产和信息安全保障的最终目的。

安天反 APT 综合解决方案由安天探海威胁检测系统、智甲终端防御系统、追影威胁分析系统组成，融合网络流量和端点检测防护能力，辅以深度鉴定环节，在网络边界、关键网段、工作站、服务器和移动终端达成部署。方案可深度检测威胁载荷和相关行为，精确检测已知恶意代码和安全风险，标定可信文件与资源，孤立未知对象和行为，结合安全可视化能力，让高级威胁无所遁形。

每周安全事件

类 型	内 容
中文标题	新型恶意软件问世 可推送银行木马服务
英文标题	New Malware Mangit Surfaces as Banking-Trojan-as-a-Service
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，安全研究人员发现了一个名为 Mangit (BKDR_MANGIT.SM) 的新恶意软件。该软件的源头是巴西地下黑客，在那里有人将其作为“银行木马服务”兜售。黑客们可以租借该木马的整套设备，租金是十天 600 美金，或者可以直接购买 Mangit 的源代码，价格大概是 8800 美金。目前，该恶意软件针对九个巴西银行，分别是花旗银行、BB 银行、Sicredi 银行、Sicoob 银行、Itau 银行、HSBC 银行、Bradesco 银行、Santander 银行和 Caixa 银行。此外，Mangit 还可以窃取 PayPal 的用户凭证和各种社交媒体账户。
链接地址	http://news.softpedia.com/news/new-malware-mangit-surfaces-as-banking-trojan-as-a-service-505458.shtml

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.Frocn.a[prv, fra]2016-06-19	该应用程序伪装成系统程序，监听通话，执行开启电话录音操作，上传录音文件，造成用户隐私泄露，建议及时卸载。（威胁等级高）
		Trojan/Android.zlewx.a[pay, fra]2016-06-20	该应用程序伪装成系统程序，运行诱导激活设备管理器，联网下载恶意子包并执行有界面安装，会自动发送扣费短信，屏蔽指定回执短信，造成用户经济损失，建议及时卸载。（威胁等级中）
		Trojan/Android.Guerrilla.d[sys, exp]2016-06-20	该应用伪装成系统应用，程序运行会隐藏图标，私自联网下载 apk 应用获取 root 权限静默安装，私自卸载指定应用，造成用户资费消耗。（威胁等级高）
		Trojan/Android.FakeBank.o[prv, exp, fra] 2016-06-22	该应用伪装成交通银行相关应用，运行后会请求激活设备管理器，获取 root 权限禁用安全软件，监听短信拦截短信，获取短信信息联网上传，根据短信内容发送指定短信，删除指定短信，造成用户隐私泄露和资费消耗。（威胁等级高）
	较为活跃的样本	Trojan/Android.FakeInst.dz[prv,rmt,exp]	该应用伪装成其他应用，运行后会请求激活设备管理器，隐藏图标，联网上传设备固件信息、本机号等信息，并获取返回的指令和参数；根据联网获取的指令执行获取用户短信、通讯录、通讯记录、安装程序列表信息、浏览器书签信息、gps 位置信息等一系列隐私信息上传到指定服务器；执行发送指定短信、拨打指定电话、下载 apk、锁屏等操作；监听短信，拦截指定号码的短信，并获取短信信息上传，造成用户隐私泄露和资费消耗。（威胁等级高）
		Trojan/Android.Hongbao.b[prv, sys]	该应用程序伪装成抢红包应用，安装无图标，后台上传用户设备、短信等隐私信息，联网获取指定短信内容，完成向用户信箱插入指定短信、修改短信替换内容等操作。建议立即卸载，避免造成隐私泄露。（威胁等级高）
		Trojan/Android.SmsThief.ah[prv, fra]	该应用伪装成中华电信，运行后隐藏图标，后台监听短信，读取短信并通过邮箱转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.E4AQQspy.g[prv, spr]	该应用伪装成 QQ 刷 svip 工具，诱导用户输入 qq 账号密码并上传到指定服务器，私自拍摄照片上传，造成用户隐私泄露和资费损耗，建议不要安装。（威胁等级中）
		G-Ware/Android.Fakegupdt.bm[exp, rog]	该应用程序伪装成系统应用，运行后联网上传手机固件信息，下载指定应用程序，还会静默卸载指定程序，存在一定安全隐患，会给用户造成一定的流量损耗，建议及时卸载该程序。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Office “组合”式漏洞攻击 CVE-2014-1761	远程攻击者可借助特制的 RTF 数据利用该漏洞执行任意代码或造成拒绝服务（内存损坏）。（威胁等级高）
	较为活跃的样本	Trojan[Backdoor]/Win32.DDOS	此威胁是一种后门木马类程序，可以连接远程服务器接受攻击者恶意操作，主要包括 DDOS 攻击和升级下载等功能。（威胁等级中）
		Trojan[Downloader]/Win32.XorCalc	此威胁是一种具有下载行为的木马类程序，运行后会释放可执行文件，访问远程服务器，下载其他恶意可执行程序，添加注册表信息和计划任务，用来执行恶意程序。（威胁等级中）
		Trojan[Backdoor]/Linux.Mayday	此威胁是一种木马类后门程序，在 linux 平台上运行，可以连接远程服务器，接受攻击者恶意操作，具体行为包括下载与更新其他恶意代码、添加删除系统文件、窃取用户敏感信息等。（威胁等级中）

比特币钓鱼活动肆虐

Chris Brook/ 文　安天公益翻译小组 / 译

近期，一些攻击者使用网络钓鱼和注册近似域名的组合方法来开展活动，旨在窃取比特币和数据区块链 (blockchain) 钱包凭证。

截至目前，这些攻击者已经注册了 100 多个假冒的比特币和数据区块链域，其中有许多模仿合法的比特币钱包。据调查，大部分网站是在 5 月 26 日注册的，近期每天还有新的网站不断冒出，这说明该活动仍然处于早期阶段。

在过去的几周，OpenDNS 安全实验室的研究人员 Artsiom Holub，Dhia Majoub 和 Jeremiah O'Connor 开始追踪 IP 地址、域名服务器和 Whois 信标之间的联系，以确定该活动的范围。

6 月初，以色列云安全公司 Cyren 发现域 blocklchain[.]info 通过 Google AdWords 的点击付费广告骗局传播，由此发现了该活动的迹象。一旦用户被诱骗访问伪造的网站 (模仿真实网站) 并登录，攻击者就会获得他们的数据区块链凭证。

Cyren 公布了研究结果，一天后，OpenDNS 进一步深入调查，发现了网站 blockchain-wallet[.]top 的钓鱼攻击。就像 Cyren 发现的网站一样，该网站与真实的 Blockchain.info 网站 (流行的比特币交易数据库) 非常相似。该网站甚至使用相同的标识和蓝绿色导航栏，现在仍然有效，不过谷歌已经将其标记为欺骗性网站，警告用户不要对其透露个人信息。

OpenDNS 还发现了类似的模糊网址 blolkchain[.]com，几天之后，它连接到同样的 IP 地址，这促使研究人员调查该 IP 地址和该范围内的类似 IP 地址。他们发现了数十个可疑的网站，其中包括多个数据区块链欺诈网站，如 wallet[.]info 和 localbitcons[.]com。

比特币地址必须用 Base58Check 编码，以避免外观相似的字符 (例如：大写字母 “O” 和数字 “0”) 之间的混淆。研究人员指出，钓鱼域严重依赖于注册近似域名，原因就在于此。如果用户在浏览器中输入网站地址时出现书写错误，就会被重定向到其他网站。

研究人员表示：“从这些例子可以很明显地看出，攻击者十分了解比特币地址的保护机制，并试图击败这些机制。”

研究人员进一步分析这些 IP 地址，它们来自同一个提供商，仅在去年，该提供商就使用了 3 个不同的名称。OpenDNS 曾指出，该提供商托管 “犯罪和恶意内容”。3 个匿名的境外托管公司利用了该公司的 IP 地址空间，兜售儿童色情、儿童模型、假冒商品，并介绍了钓鱼网站、数据区块链和 iCloud 相关的内容。

该公司的名称本来是 Ecatel，以前它的总部设在荷兰。后来，它更名为 QUASINETWORKS，并于 2015 年 12 月搬到了塞舌尔。今年 4 月，它更名为 Novogara。

研究人员交叉引用托管域和 IP 地址的 Whois 注册信息，确定了用于注册数据区块链欺诈域的 6 个不同的电子邮件地址。目前，这些电子邮件地址仍然被用于注册域。

研究人员在博客中说：“通过调查 IP 地址空间、域名服务器和 Whois 信标，我们发现了犯罪分子回收其基础设施和资源的频率，说明他们严重依赖于防弹境外托管服务提供商来传播恶意软件和钓鱼活动。”

现在，人们对加密货币兴趣盎然，上述攻击就是在这种条件下出现的。在过去的几个月里，比特币的价格扶摇直上，很多人将这一趋势与勒索软件的肆虐联系了起来。当受害者遭到勒索软件攻击者的勒索时，通常被要求以比特币支付赎金。在这种情况下，攻击者往往会指导用户购买比特币，以便受害者换取解密密钥。钥匙的价格高低不一，以上周发现的勒索软件 RAA 为例，用户被要求支付 0.39 比特币 (250 美元) 来解锁文件，而本月初发现的勒索软件 Black Shades 只要求 0.07 比特币 (30 美元) 来解锁文件。

OpenDNS 指出，面对这种局面，钱包企业应加强他们的安全措施，以防止类似的钓鱼活动和注册近似域名攻击。

原文名称	Bitcoin Phishing Campaign Uncovered
作者简介	Chris Brook，《Threatpost》副编辑。
原文信息	2016 年 6 月 21 日《Threatpost》发布，原文地址 https://threatpost.com/bitcoin-phishing-campaign-uncovered/118799/
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《一款利用 Windows 组件复活的木马分析报告》

近日，安天追影小组在持续追踪网络犯罪的过程中，发现一款利用 Windows 操作系统中的 BITS 服务组件来下载运行恶意程序的特殊木马。

BITS 是后台智能传送服务的简称，作为一个底层而且可靠的传送服务，它可以在后台进行异步文件传输，一般在操作系统的更新中会使用到它，有些第三方应用程序也会使用该组件来处理文件传输。不幸的是，一些攻击者也开始滥用这个服务来下载执行一些恶意程序，以达到绕过系统防火墙的拦截以及安全软件的监控和查杀的目的。

经分析发现，通过一定方法向 BITS 服务注册下载任务时，可以导致 BITS 自动下载文件，而它的一些特性又允许自身执行下载好的文件，从这方面来看，BITS 的行为与下载者相似。

攻击者通过利用 BITS 服务提供的这些特性，无需修改文件或者注册表项就可以下载执行恶意程序，即不需要在磁盘上留有充当下载者的木马文件，这也使得传统安全软件很难对其进行查杀。而且，即便是一些安全软件可以识别并删除原始木马文件，受害用户电脑上的恶意网络流量依然会处在活跃状态，也就是说 BITS 服务在后台仍然可以不受干扰的继续下载恶意程序。当恶意程序下载完成后，BITS 服务还会运行它，新的恶意程序又会被重新安装在用户电脑上。

为了应对上述威胁，安天追影小组提醒广大用户不要随意运行来历不明的应用程序，使用 Win7 或更新版本的操作系统，开启 UAC(User Account Control，即用户帐户控制，是微软为提高系统安全引入的技术，它要求用户在执行可能会影响计算机运行的操作或执行更改影响其他用户的设置的操作之前，提供权限或管理员密码，可以帮助用户防止恶意软件和间谍软件在未经许可的情况下在计算机上进行安装或对计算机进行更改），同时要及时更新杀毒软件。

木马程序

安天【追影威胁分析系统】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。

文件名	1E9A1B219D0347016D435656D04FCB42
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	379 KB
MD5	1E9A1B219D0347016D435656D04FCB42
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.ZlobBits
判定依据	智能学习

危险行为

行为描述	危险等级	行为描述	危险等级
延时	★★★	绕过监控设置自启动	★★★★

最终依据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：延时、绕过监控设置自启动、获取系统版本、查找指定内核模块、添加计划任务、连接网络、创建特定窗体、自启动、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。

其他行为

行为描述	危险等级	行为描述	危险等级
获取系统版本	★	查找指定内核模块	★
添加计划任务	★	连接网络	★
创建特定窗体	★	自启动	★
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	★

文件操作

操作	文件路径
删除	c:\windows\tasks\{c6eeac39-af88-6102-2daf-968b2666157f}.job
删除	c:\windows\tasks\{c6eeac39-af88-6102-2daf-968b2666157f}.job

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=1E9A1B219D0347016D435656D04FCB42