安天周观察

主办：安天　2016 年 1 月 25 日（总第 26 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天 CERT 发布

《2015 年网络安全威胁的回顾与展望》

近日，安天 CERT 发布了“观点型年报”《2015 年网络安全威胁的回顾与展望》，围绕五个主题总结了 2015 年的网络安全威胁形势，并对 2016 年的新形势做出了预测。

高级持续性威胁 (APT) 的层次分化

在 2015 年 APT 事件中，超级 APT 组织拥有大量 0day 漏洞和豪华的攻击装备储备；而一些攻击组织则利用现有平台和商用木马来完成的攻击事件；但也有一些技术相对粗糙，手段亦不高明的攻击事件也同样体现出攻击方持续和定向攻击作业的特点。因此，从技术能力、资源储备、攻击手段等方面综合考虑，安天将 APT 攻击能力细分为 A2PT(“高级的”APT)、APT、准 APT、轻量级 APT 几个等级。

非法泄露的数据和隐私正在汇入地下经济的基础设施

2015 年，由网络攻击引发的数据泄露事件依旧猖獗，拖库攻击、终端木马和 APP 的超量采集、流量侧的信息劫持获取，已经成为数据泄露的三个主要渠道。信息泄露的背后已经形成了一条完整的利益链，这些用户信息或被用于团伙诈骗、钓鱼，或被用于精准营销。同时，随着黑产的规模化，这些数据将持续汇入黑产的“基础设施”当中，从而使其可能具备超越公共安全和安全厂商的资源能力，而且也不排除这种地下基础设施摇身一变，以“威胁情报”的形式，同时为黑产和白帽子服务。

用户需要负责任的漏洞披露机制和更细腻的漏洞应急指导

业内对严重漏洞的预判能力正在下降，从 2014 年的“心脏出血 (HeartBleed)”、“破壳 (Bash Shellshock)”，到 2015 年的“幽灵 (Ghost)”，都给人以措手不及感，而在漏洞出现后的快速跟进中，业内反而开始逐步丧失耐心指导用户止损和进行精细处置的应急传统。但这些工作尽管并不吸引眼球，却对于机构、行业用户来说具有更有效的价值。

勒索软件引领 PC 恶意代码威胁关注度，成为用户的噩梦

在 2015 年 PC 平台恶意代码行为分类排行榜中 (HASH)，备受关注的勒索软件位列第九位。安天 CERT 在 2015 年先后发布了《揭开勒索软件的真面目》和《邮件发送 JS 脚本传播敲诈者木马的分析报告》，详细地揭露了勒索软件的传播方式、勒索形式、历史演进以及相应的防御策略。

威胁将随“互联网 +”向纵深领域扩散与泛化

在 2015 年，这种安全威胁泛化已经成为常态，安天以一张图表来说明 2015 年威胁泛化的形势。

2016 年网络安全形势预测

安天预测威胁情报的共享体系，同样使其具有了很大被污染的可能性。“上游厂商”将遭受更多的攻击，导致整个供应链、工具链的脆弱性增加。同时，随着中国政府以“互联网 +”盘活传统产业的努力，中国所面临的安全威胁也将向传统的工业和基础设施中快速逼近。

由于安天 CERT 的部门分工所决定的分析视野的不同，本年报涉及到的移动安全相关内容较少，安天移动安全公司 (AVL TEAM) 后续会单独发布移动安全年报。（全文地址：http://www.antiy.com/response/2015_Antiy_Annual_Security_Report.html）

安天参加山西省信息网络安全高峰论坛并发表演讲

1 月 19 日，山西省信息网络安全高峰论坛在太原召开，会议由山西省网络安全协会主办，国家信息中心信息安全研究与服务中心山西分中心主任郭子龙主持。来自山西省网信办、公安厅等政府主管部门及安天、华为、深信服等多家安全厂商总计约 200 人参加了会议。

本次会议围绕着“网络安全综合防御”、“移动电子政务安全”、“APT 攻击检测与防御”等主题展开，邀请到数位业内专家发表演讲。其中，安天副总工程师李柏松发表了题为《弹道有痕——中国面临的 APT 攻击的风险与案例分析》的报告。报告以“震网”、“HangOver”、“方程式”和“APT-TOCS”等具有代表性的 APT 攻击事件为例，指出我国当前面临的网络安全威胁形势与挑战，并根据 APT 攻击的典型过程，结合安天在具体实践经验，讨论了如何转换安全思路，从内网深度检测、前置沙箱分析、利用白名单 + 安全基线、网络监控和数据集中分析等多个角度，建立新的布防点和体系化防御。

每周安全事件

类 型	内 容
中文标题	俄罗斯驻以色列使馆网站被黑 黑客张贴土耳其国旗
英文标题	Russian Embassy in Israel Website Hacked– Hackers Post Turkish Flag
作者及单位	Waqas，HackRead
内容概述	近日，来自亲土耳其阿塞拜疆的黑客组织 Börteçine Siber Tim 对俄罗斯驻以色列使馆网站 (russianembassy.org.il) 进行了一次有针对性的攻击。遭受攻击的使馆网站保留下来的页面的谷歌缓存没有显示任何俄罗斯对以色列的外交议程，只有土耳其的国旗图和国父凯末尔 (穆斯塔法·凯末尔·阿塔图尔克) 的形象。另外该黑客组织在去年 12 月攻击了 Russian Communications 俄罗斯通讯与 Mass Media 大众传媒的部长尼古拉·尼基福罗夫的 Instagram 账号以及莫斯科 Lokomotiv 足球俱乐部的官方网站。而另一家土耳其组织 THT 则于去年十一月进行了对 Russian Central Bank 的 DDoS 攻击，当时迫使该银行网站下线超过 10 分钟。
链接地址	https://www.hackread.com/russian–embassy–in–israel–website–hacked–with–turkish–flag

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	Trojan/Android.Avtolic.a[prv，spy] 2016–01–18	该应用程序开机自启，运行上传手机固件信息、短信箱、通讯录等隐私信息，后续可以通过接收短信指令完成上传以上隐私操作，还会执行电话录音操作，并上传录音文件，会造成用户隐私泄露和资费消耗，建议及时卸载该程序。(威胁等级中)
		Trojan/Android.ouradwaretv.a[sys] 2016–01–18	该应用伪装视频解码插件，安装无图标，开机自启，激活设备管理器，包含下载安装 apk，锁定屏幕等恶意代码，可能会影响用户体验，但运行后并未触发该行为，am 命令触发，建议用户卸载。(威胁等级中)
		RiskWare/Android.Vshare.a[exp] 2016–01–19	该应用程序包含风险代码，安装运行之后会在通知栏推送应用信息，并拥有静默安装应用的功能，建议谨慎使用。(威胁等级中)
		Trojan/Android.xlnet.a[spr，fra，exp] 2016–01–20	该应用伪装成系统应用，运行后激活设备管理器，隐藏图标，遍历联系人，群发诈骗短信，可能造成用户资费损耗，建议卸载。(威胁等级中)
		Trojan/Android.crittercism.a[prv，spy] 2016–01–21	应用伪装系统应用，点击配置后隐藏图标，通过远端 ftp 控制用户手机执行窃取用户短信、联系人、位置信息、手机图片、手机视频、对手机截屏、通话录音、调用摄像头拍照等功能，建议用户立即卸载。(威胁等级低)
		G–Ware/Android.fakewechat.a[fra，rog] 2016–01–22	该应用伪装成微信应用，包含投注的功能，可能用于违法赌博交易，建议谨慎使用。(威胁等级中)
	较为活跃的样本	Trojan/Android.FakeBank.k[prv，exp]	该应用伪装银行应用，运行后诱骗用户激活设备管理器，加载钓鱼网页，强行中止安全软件的运行，同时拦截来自银行的短信，对用户的资金安全造成威胁，建议用户立即卸载。(威胁等级中)
		Trojan/Android.Androrat.g [prv，rmt，spy]	该应用伪装成系统应用，运行后隐藏图标，接收远程指令，获取地理位置信息、通话记录、录音文件、短信等；同时私自下载应用、删除文件、开启 wifi、自我卸载，可能造成用户隐私泄露和资费损耗，建议卸载。(威胁等级中)
		Trojan/Android.AutoSMS.i[exp]	该应用程序运行会私自向指定号码发送短信，包含拨打电话风险代码，有造成用户资费消耗的风险，建议卸载。(威胁等级中)
		G–Ware/Android.Fakegupdt.au [rog，exp]	该应用伪装成系统应用，安装无图标，运行后会加载广告，造成用户资费损耗，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	Linux 内核 CVE–2016–0728	CVE–2016–0728 是个 Linux 内核漏洞，本地用户可利用这个漏洞提升到 root 权限。研究人员认为，上千万台 Linux 个人电脑、服务器，以及 66% 的安卓手机和平板设备面临威胁。(威胁等级高)
	较为活跃的样本	Trojan[Downloader]/Win32.Delf.ahb	此威胁是使用 delphi 语言编写具有下载行为的木马类程序，运行后会连接网络并下载其他恶意程序执行。通过以邮件、挂马、捆绑正常软件来进行传播。(威胁等级中)
		GrayWare[AdWare]/ Win32.InstallMonster.do	此威胁是广告件类程序，主要行为是进行广告件程序的安装，在安装成功后除其正常应用外，还会窃取用户的各种上网行为等敏感信息。(威胁等级中)
		Trojan[Ransom]/Win32.PornoAsset.ae	此威胁是一种勒索木马类程序，主要通过勒索用户使其制作者获利。勒索类的木马一般通过下载或系统漏洞感染用户系统。部分勒索木马在运行时加密用户的数据，用户支付赎金给软件制作者后才能解密数据。(威胁等级中)

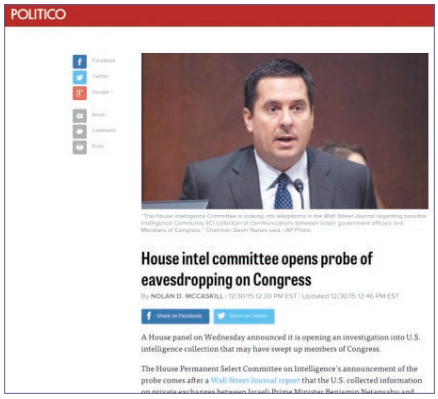
窥探国会和以色列：NSA 监控项目拥护者自掘坟墓

Glenn Greenwald/ 文　安天公益翻译小组 / 译

《华尔街日报》近日的报道称，NSA(美国国家安全局) 监控以色列总理本雅明·内塔尼亚胡和他的高级助手。众议院情报委员会长共和党主席，NSA 监控项目拥护者皮特·胡克斯特拉得知了这一窃听事件，非常愤慨。但在 2014 年 1 月，我与众议员胡克斯特拉辩论 NSA 的监控项目，他对我提出的隐私担忧极尽嘲讽和不屑一顾。“监控是一个事实”，他嗤之以鼻。当然，这一切发生在胡克斯特拉知道他和他的以色列朋友们被监控之前。

现在，他得知他和战友们的隐私遭到了侵犯，他就不再那么傲慢了。事实上，他是如此的愤怒，这位长期的 NSA 拥护者甚至要求对监控他和他的朋友们的 NSA 和政府官员提起刑事起诉。这种模式 (强烈支持政府监控项目的政治官员一旦得知自己被窥探，一夜之间变成讨伐监控项目的隐私倡导者) 已经重演了一遍又一遍。在斯诺登爆料之后，经常可以看到外国政府反应冷漠，直到他们得知他们自己，而不仅仅是他们的目标，也被监控了。

所以，《华尔街日报》的报道发布后，我们看到，多年来赞同和负责 NSA 大规模监控项目，甚至对此睁一只眼闭一只眼的很多人突然大力反对了。因为他们自己或者他们喜欢的外国官员都被卷入了这个监控网，因此难以抑制自己的愤怒。一夜之间，隐私具有了最高的价值，因为他们的隐私 (而不仅仅是平民的) 遭到了侵犯。


POLITICO

House intel committee opens probe of eavesdropping on Congress

By NOLAN D. MCCASKILL | 12/30/15 12:30 PM EST | Updated 12/30/15 12:46 PM EST

A House panel on Wednesday announced it is opening an investigation into U.S. intelligence collection that may have swept up members of Congress.

The House Permanent Select Committee on Intelligence's announcement of the probe comes after a Wall Street Journal report that the U.S. collected information

之前，这些拥护者大肆宣扬：只要你没做坏事，那么你有什么好隐瞒的。现在他们怎么态度大变呢？他们说的话是否仍然适用？抑或是，他们知道自己做了坏事，因此对被监控感到非常恼怒？

我一直认为，在间谍事件上，披露针对外国领导人的监控是最不重要的，因为这是最合理的间谍活动类型。正如我在我 2014 年的书中所说的，“相对于针对民众的大规模监控项目，那些披露并不怎么重要”，因为“数百年间，各国相互窥探元首，其中包括友邦。”但是，NSA 不仅监听内塔尼亚胡和他的高级助手的谈话，还无证窃听了一名国会议员。

NSA 将无证窃听称为“无意收集”。NSA 在无证监控美国公民的谈话时，用的正是这一术语，但声称这些美国人没有被“作为目标”，而是恰巧正在与 NSA 的外国目标之一通话。

“无意收集”的说法一直旨在掩盖一个事实：NSA 确实在无任何形式的搜查令的情况下频繁地窥探美国公民的谈话。事实上，正如我在本文中介绍的，美国国会制定的 2008 年 FISA(《涉外情报监控法》) 的其中一个主要和明确的目的是：允许 NSA 在无任何形式的搜查令的情况下窃听美国公民的谈话。“2008 年法律的主要目的是：允许美国政府收集美国公民的国际通信，而且不需证明通信的任何一方是否在做违法的事。”美国公民自由联盟的贾米尔·杰弗说，“政府的很多宣传都是为了掩盖这个事实，但这是一个关键问题：政府不需要‘针对’美国人就能收集他们的海量通信。”

不管您有什么样的看法——也就是说，即使您认为，NSA 无证监听美国公民和国会成员的私密谈话没什么不对，但是这突如其来的、自私自利的隐私权拥护着实令人作呕。无证监听没有做任何坏事的人们 (有史以来最大的非嫌犯大规模监控系统) 本质上是权力滥用和不公正的，我们不需要做这样一个报告来告诉全世界本杰明·内塔尼亚胡和皮特·胡克斯特拉被监控了，因为大家对此早已心知肚明。

原文名称	Spying on Congress and Israel: NSA Cheerleaders Discover Value of Privacy Only When Their Own Is Violated
作者简介	Glenn Greenwald，记者、律师和作家。
原文信息	2015 年 12 月 31 日《The Intercept》原文地址 https://theintercept.com/2015/12/30/spying-on-congress-and-israel-nsa-cheerleaders-discover-value-of-privacy-only-when-their-own-is-violated/
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《QQ 粘虫分析报告》

近日，安天追影小组从威胁感知平台发现一个盗取 QQ 号的样本，其关联生成器“QQ 粘虫盗号生成器”，主要功能为盗取 QQ 号。在运行“生成器”时只需填写“收信邮箱地址”。“信”是一个黑产术语，在 QQ 黑产中，一组 QQ 用户名和密码称为一个“信”。在之前的分析中，特别是手机拦截马等采用 SMTP 发信都需要发件邮箱的帐号和密码才能登录发送邮件，而本次分析的 QQ 盗号木马采用了第三方邮件发送服务，可以随意伪造发信邮箱，无需发信邮箱的帐号和密码信息。

样本行为简要分析

追影小组经分析发现该木马的工作流程如下：在已登录 QQ 的设备上运行样本后，桌面弹出 QQ“重新登录”窗口，让用户误以为账号安全问题需要重新输入密码，输入密码后，该窗口连续弹出两次，用户三次输入的密码均以邮件的形式发送到收信邮箱，弹出三次的目的也是为了防止密码输入错误导致密码盗取失败。

通过收信邮箱收到的邮件以及网络分析可以发现，木马发送邮件是以第三方平台“http://tool.chacuo.net/mailanonymous”伪造发件人方式向收信邮箱发送邮件，这种方式可以不需要使用 smtp 发邮件，从而不需要邮箱账号密码登录，不会暴露黑客的邮箱登陆信息。伪造的发件人邮箱以 @VIP.com 结尾，模仿 QQ VIP 邮箱，经过对不同版本生成器生成的样本分析发现，伪造的发件人邮箱分别为 QQ@VIP.com 和 QQ10369323@VIP.com。

黑客组织信息

通过生成器中出现的“千里眼工作室客服 QQ：10369323”等字样，可得知该木马制作者是有组织有规模的团队，搜索该 QQ 号发现其主要盈利途径为出售 VIP 版免杀生成器，并且将其免费版本 (多种不同版本) 发布在网盘、论坛等多种平台，来吸引更多的客户，该 QQ 号的密保手机为 178******51。

总结

目前，QQ 聊天工具已不仅具有聊天功能，其游戏等各种付费业务，促使盗取 QQ 号成为黑产的一个成熟业务。QQ 粘虫的盗号方式，相对成本较低，盗号效果也不错，在利益的驱使下，促使其成为有规模的团队，经过与杀软的不断对抗，升级，后续还会有新的方式等待网络犯罪分析来发现。

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、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、美国软件交叉索引 (NSRL) 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、静态分析鉴定器将文件判定为木马程序。该文件具有以下行为：创建腾讯相关窗口，谨防盗号、钓鱼类木马；Trojan[GameThief]/Win32.Lmir.axv；获取系统版本；遍历进程；创建特定窗体；查找指定内核模块；连接网络；连接特殊 URL；请求加载驱动的权限；获取 socket 本地名称；获取驱动器类型；查找特定窗体；获取计算机名称；获取主机用户名称。

文件名	211DD401D89DB29BCF8CFECDC274AB8D
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.74 MB
MD5	211DD401D89DB29BCF8CFECDC274AB8D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[GameThief]/Win32.Lmir.axv
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=211DD401D89DB29BCF8CFECDC274AB8D

◆ 危险行为

行为描述	危险等级
创建腾讯相关窗口，谨防盗号、钓鱼类木马	★★★
Trojan[GameThief]/Win32.Lmir.axv	★★★★

◆ 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	★★	遍历进程	★
查找指定内核模块	★	创建特定窗体	★
连接特殊 URL	★	连接网络	★
获取驱动器类型	★	请求加载驱动的权限	★
获取计算机名称	★	获取 socket 本地名称	★
获取主机用户名称	★	查找特定窗体	★