网络安全信息简报

安博士月刊

2014.01（Vol.15）

2014 年网络安全 7 大预测

2014年网络安全7大预测

无止境的网络攻击 ‘多样化·高级化·加速化’

回顾2013年全球网络空间，可谓是冲突不断、状态百出。大规模的安全事件之频频发生，如震惊世界的韩国黑客入侵事件[1]，还有通过移动设备试图入侵的恶意代码的事件也呈上升趋势。除了针对特定组织进行复杂且多方位的网络攻击的APT（Advanced Persistent Threat，高级持续性威胁）攻击的增加，面向不特定目标的狂轰滥炸式的恶意软件传播也同时进行。纯粹娱乐性的黑客袭击时代早已过去，现在我们面临的则是个人信息或企业和国家重要信息遭到窃取的重大问题。黑客窃取金融信息谋取经济利益，或泄漏企业的核心技术，还有监视国家核心人事信息。而窃取国家重要信息时使用的技术更是高级和精致。

黑客攻击已不只限于一个目标，个人和组织、国内和国外、特定和不特定、软件和硬件都成为了黑客的攻击对象。尤其在2013年的安全市场显示了该界线被瓦解的局面，2014年该局面更是深化。下面，让我们看一下安博士的网络安全专家们发布的2014年7大安全预测。

1. APT攻击的高级化，攻击范围不断扩大

2013年出现的恶意代码大部分使用了擅自更改一般用户的系统信息后，引导用户访问伪造的假金融网站，窃取用户的金融信息的手法。另外，盗取游戏币的在线游戏黑客手法和盗取金融信息的黑客手法越来越相似，致使无法区分两者。而且，黑客通过植入的恶意代码窃取金融信息的攻击的事件频繁发生，由此可见，黑客制作恶意代码的目的演变为谋取经济利益。

从用在盗取信息的两种恶意代码种类的功能和目的的变化来看，今后出现的大部分的恶意代码与APT攻击非常相似，或者是以融合的形式出现。因此，在2014年，不仅针对特定目标的APT攻击将继续，而且攻击范围将不断扩大。

另外，传统的APT攻击和水坑式(Watering-Hole)攻击的界线已越来越模糊。特别是，有可能出现为了经济利益大量传播恶意代码并试图比特币开采(Bitcoin mining)的恶意软件。

2. 电子金融诈骗和网络犯罪的产业化

在2013年，利用恶意软件的电子金融诈骗主要使用网络钓鱼(Phishing)、域欺骗(Pahrming)、电话诈骗(voice phishing)、短信钓鱼(Smishing)和内存黑客(Memory hacking)等攻击手法窃取金融信息。窃取个人金融信息和存款而使用的恶意代码技术变得越来越高级和精确。黑客制作恶意代码已不再是为了炫耀自己的实力，而是作为盗取经济利益的重要工具，在网上进行交易，并利用在网络犯罪的产业化。

在2014年，黑客们将继续通过应用程序漏洞、伪造正常的程序和利用U盘之类的存储设备等方式传播恶意代码。而且，对特定金融服务，如网上银行等的攻击也会增加。

1 韩国黑客入侵事件。分别是，3月20日发生的韩国多家银行和电视台遭遇具有典型APT特征攻击和6月25日发生的针对政府和公共机关的DDoS攻击事件。

3. 恶意代码传播方式的多样化和高级化

在2014年，恶意代码传播方式将更加多样且高级。目前为止，通过更新漏洞和鱼叉式网络钓鱼等方式，向不特定对象传播大量恶意代码，并根据目的传播变种的恶意代码。在2014年，除了传统的方式，很有可能出现大量传播恶意代码的新的方式。比如，通过多数用户访问的内容分发网络（CDN）、域名管理企业或互联网提供商（ISP）发布大量恶意代码的攻击方式将会增加。 因此，在2014年，互联网服务企业更加需要注意。

4. 随着Windows XP 即将结束支持，安全威胁增加

随着Windows 8.1 正式发布，微软公司再次强调将在2014年4月中止Windows XP 安全更新，也就是不再为XP漏洞提供补丁。那么今后Windows XP 用户从理论上来讲将永难脱遭受“零日漏洞”攻击的可能。因此，支持结束以后对于安全威胁的防御纯粹依赖于防病毒软件、防火墙等计算机安全解决方案。

目前Windows XP不支持 IE9以上的版本，主要使用易受恶意代码攻击的IE6~8版本。数据显示，全球范围内XP的市场份额约占25%，而中国的XP市场份额更高达70%，个人用户安装和使用XP的计算机将近2亿台。 与此同时，一些重要信息系统和企业级用户也在大量使用XP系统。如果XP被黑客发现严重漏洞又无法打补丁，广大网民和企事业单位电脑都将面临木马病毒感染、敏感信息泄露，甚至业务系统和生产系统无法正常运行的风险。因此，Windows XP用户在结束支持之前需要升级到Windows 7或 Windows 8。

5. 监视特定对象的移动间谍软件的增加

2013年，通过社交网络和移动社交网络伪装成周岁宴、结婚请帖、快递和信用卡清帐内容的移动短信钓鱼恶意软件广泛传播。该恶意代码是将相同的应用程序发布给多数的用户的目的而制作，并公开发布，因此很容易就被发现。

但是，如果移动短信钓鱼恶意软件以盗取特定企业的机密信息为目的制作的话，它的存在不会轻易被发现。尤其是，经常携带并存有很多个人和业务信息的智能手机就被黑客们视作绝佳的漏洞挖掘平台。预计在2014年，通过智能手机传播恶意代码并监视特定对象或窃取信息的间谍软件也将增加。

6. 对网络信息的国家意识转换

2013年，爱德华•斯诺登向世界曝光美国国家安全局(NSA)监控项目。还发生了特定国家试图窃取以美国为据点的企业和最少141个机关的重要信息等国家之间的收集信息事件。随着针对国家的诸多窃听和监听的事件被暴，国家之间的网络战争越来越精确和加速。

因此，为了减少网络攻击和数据泄漏的损害，需要加密技术和更为先进的安全技术。

7. 试图植入恶意代码到BIOS和固件中

2013年4月，发生了制作BIOS厂家的源代码被泄漏的事件。10月，发生了某企业的路由固件被植入了后门程序的事件。如平板电脑之类的电子设备通过下载制造商分发的固件进行更新，但是无法保证制造商彻头彻尾地管理从研发到分发的过程。像这样，通过硬件中嵌入的软件进行恶意行为的可能性也呈上升趋势。为了植入恶意代码到BIOS或固件，需要制作商蓄意制作，或是有内部有同谋。又或者，攻击者入侵到内部系统后植入恶意代码。虽然这个可能性非常低，但是如果植入成功很难被发现。特别是，国家之间的网络攻击的存在渐渐被人们所知，怀疑不仅是网络犯罪分子就连国家机关也为收集信息而利用硬件制造商。

虽然植入恶意代码的过程不是简单的事情，因此不会暴增，但是预测2014年黑客将试图植入恶意代码到硬件或固件后进行恶意攻击。

http://www.ahn.com.cn
http://global.ahnlab.com
http://www.ahnlab.com

关于安博士（AhnLab,Inc.）

安博士的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

安博士已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区酒仙桥甲12号电子城科技大厦1206室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0935 / +86 21 6095 6780 | v3site@ahn.com.cn