11 2012 年网络安全挑战与工作展望

■ 2012 年值得关注的网络安全热点问题

随着我国互联网新技术、新应用的快速发展，2012 年的网络安全形势将更加复杂，尤其需要重点关注如下几方面问题：

（一）网站安全面临的形势可能更加严峻，网站中集中存储的用户信息将成为黑客窃取的重点。由于很多社交网站、论坛等网站的安全性差，其中存储的用户信息极易被窃取，黑客在得手之后会进一步研究利用所窃取的个人信息，结合社会工程学攻击网上交易等重要系统，可能导致更严重的财产损失。

（二）随着移动互联网应用的丰富和 3G、wifi 网络的快速发展，针对移动互联网智能终端的恶意程序也将继续增加，智能终端将成为黑客攻击的重点目标。由于 Android 手机用户群的快速增长和 Android 应用平台允许第三方应用发布的特点，运行 Android 操作系统的智能移动终端将成为黑客关注的重点。

（三）随着我国电子商务的普及，网民的理财习惯正逐步向网上交易转移，针对网上银行、证券机构和第三方支付的攻击将急剧增加。针对金融机构的恶意程序将更加专业化、复杂化，可能集网络钓鱼、网银恶意程序和信息窃取等多种攻击方式为一体，实施更具威胁的攻击。

（四）APT[18]攻击将更加盛行，网络窃密风险加大。APT 攻击具有极强的隐蔽能力和针对性，传统的安全防护系统很难防御。美国等西方发达国家已将 APT 攻击列入国家网络安全防御战略的重要环节，2012 年 APT 攻击将更加系统化和成熟化，针对重要和敏感信息的窃取，有可能成为我国政府、企业等重要部门的严重威胁。

（五）随着 2012 年 ICANN 正式启动新通用顶级域名（gTLD）业务，新增的大量 gTLD 及其多语言域名资源，将给域名滥用者或欺诈者带来更大的操作空间。

（六）随着宽带中国战略开始实施，国家下一代互联网启动商用试点，以及无线城市的大规模推进和云计算大范围投入应用， IPv6 网络安全、无线网安全和云计算系统及数据安全等方面的问题将会越来越多地呈现出来。

[18]APT 即高级可持续威胁（Advanced Persistent Threat），也称为定向威胁，指某组织对某一特定对象展开的持续有效的攻击活动和威胁。这种攻击活动具有极强的隐蔽性和针对性，通常会运用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击。黑客个人的行为一般不能构成 APT 攻击，因为通常情况下没有足够的资源来开展这种先进且复杂的攻击活动。

■ 对策建议

随着 2012 年下一代互联网和宽带中国战略的推进，为保障国家网络空间安全，维护互联网的健康环境，保护网民权益，我国政府主管部门、互联网企业和互联网用户应进一步重视网络安全问题，共同提高网络安全水平。建议政府部门尽快制定出台我国的国家网络安全战略，为各部门开展网络安全工作指明方向。建议立法和执法部门加大网络犯罪立法、惩治和量刑力度，形成有效震慑。建议互联网主管部门加大网络安全行政监管力度，增强对互联网信息和增值业务服务商的管理。建议互联网相关产品厂商加强对产品安全性的管理和规范，及时发布漏洞补丁和更新版本。建议网站和信息系统强化系统的安全防护，提高网络安全监测和应急处理能力，并加强相关人员队伍的建设。建议电信运营企业完善网络安全监测和应急体系建设，提高网络攻击发现和溯源处置能力。建议广大网民要提高对网络安全威胁的认识及网络安全防护意识，做好漏洞修补和恶意程序查杀等防护措施。

12 网络安全术语解释

- 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成的以处理信息和数据为目的的系统。

- 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

- 恶意程序

恶意程序是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。恶意程序分类说明如下：

1. 特洛伊木马（Trojan Horse）

   特洛伊木马（简称木马）是以盗取用户个人信息，甚至是远程控制用户计算机为主要目的的恶意程序。由于它像间谍一样潜入用户的计算机，与战争中的“木马”战术十分相似，因而得名木马。按照功能，木马程序可进一步分为：盗号木马[19]、网银木马[20]、窃密木马[21]、远程控制木马[22]、流量劫持木马[23]、下载者木马[24]和其它木马六类。

2. 僵尸程序（Bot）

   僵尸程序是用于构建大规模攻击平台的恶意程序。按照使用的通信协议，僵尸程序可进一步分为：IRC 僵尸程序、Http 僵尸程序、P2P 僵尸程序和其它僵尸程序四类。

[19] 盗号木马是用于窃取用户电子邮箱、网络游戏等账号的木马。
[20] 网银木马是用于窃取用户网银、证券等账号的木马。
[21] 窃密木马是用于窃取用户主机中敏感文件或数据的木马。
[22] 远程控制木马是以不正当手段获得主机管理员权限，并能够通过网络操控用户主机的木马。
[23] 流量劫持木马是用于劫持用户网络浏览的流量到攻击者指定站点的木马。
[24] 下载者木马是用于下载更多恶意代码到用户主机并运行，以进一步操控用户主机的木马。

3. 蠕虫（Worm）

蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的的恶意程序。按照传播途径，蠕虫可进一步分为：邮件蠕虫、即时消息蠕虫、U 盘蠕虫、漏洞利用蠕虫和其它蠕虫五类。

4. 病毒（Virus）

病毒是通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的恶意程序。

5. 其它

上述分类未包含的其它恶意程序。

随着黑客地下产业链的发展，互联网上出现的一些恶意程序还具有上述分类中的多重功能属性和技术特点，并不断发展。对此，我们将按照恶意程序的主要用途参照上述定义进行归类。

- 僵尸网络

僵尸网络是被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为，如可同时对某目标网站进行分布式拒绝服务攻击，或发送大量的垃圾邮件等。

- 拒绝服务攻击

拒绝服务攻击是向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务。

- 网页篡改

网页篡改是恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

- 网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息，诱骗用户访问钓鱼网站，以获取用户个人秘密信息（如银行帐号和帐户密码）。

- 网页挂马

网页挂马是通过在网页中嵌入恶意程序或链接，致使用户计算机在访问该页面时被植入恶意程序。

- 网站后门

网站后门事件是指黑客在网站的特定目录中上传远程控制页面从而能够通过该页面秘密远程控制网站服务器的攻击事件。

- 垃圾邮件

垃圾邮件是将不需要的消息（通常是未经请求的广告）发送给众多收件人。包括：（一）收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；（二）收件人无法拒收的电子邮件；（三）隐藏发件人身份、地址、标题等信息的电子邮件；（四）含有虚假的信息源、发件人、路由等信息的电子邮件。

- 域名劫持

域名劫持是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假 IP 地址或使用户的请求失败。

- 非授权访问

非授权访问是没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中，黑客利用专门的漏洞利用程序（Exploit）来获取信息系统访问权限。

- 路由劫持

路由劫持是通过欺骗方式更改路由信息，以导致用户无法访问正确的目标，或导致用户的访问流量绕行黑客设定的路径，以达到不正当的目的。

编者按：

谢谢您阅读国家互联网应急中心《2011 年中国互联网网络安全报告》，如果您发现本报告存在任何问题，请您及时与我们联系，电子邮件地址为：cncert@cert.org.cn。我们对此深表感谢。