第37卷 第22期
Vol.37 No.22

计 算 机 工 程
Computer Engineering

2011年11月
November 2011

• 专栏 •

文章编号：1000—3428(2011)22—0001—04 文献标识码：A 中图分类号：TP309

一种基于 Android 系统的手机僵尸网络

刘潇逸[1,2]，崔 翔[2]，郑东华[3]，李 善[3]

(1. 华东师范大学计算机科学技术系，上海 200241；2. 中国科学院计算技术研究所，北京 100080；
3. 上海市经济和信息化委员会信息中心，上海 200003)

摘 要：提出一种基于 Android 系统的手机僵尸网络，设计命令控制信道及手机状态回收方式。分析僵尸手机的恶意行为，给出手机僵尸网络防劫持策略，包括多服务器策略、域名 flux 技术与身份认证系统，通过 RSS 及 GZIP 压缩技术降低僵尸程序消耗的网络流量。对手机僵尸网络的发展趋势及防御手段进行了讨论。

关键词：手机僵尸网络；Android 系统；命令控制信道；恶意行为；防劫持；流量控制

Mobile Botnet Based on Android System

LIU Xiao-yi[1,2], CUI Xiang[2], ZHENG Dong-hua[3], LI Shan[3]

(1. Department of Computer Science and Technology, East China Normal University, Shanghai 200241, China;
2. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China;
3. Information Center, Shanghai Municipal Commission of Economy and Informatization, Shanghai 200003, China)

【Abstract】This paper proposes a kind of mobile botnet based on Android system, including the design of command and control channel, the way that botmaster recycles the information of controlled phones. It analyzes the malicious act of the bot phones, gives the defense of hijack, including the multiserver strategy, the domain-flux technology, and the identity authentication system. It reduces the flow rate of bot program by RSS and GZIP technology. The future and the defense of mobile botnet are discussed.

【Key words】mobile botnet; Android system; command and control channels; malicious act; defense of hijack; flow control

DOI: 10.3969/j.issn.1000-3428.2011.22.001

1 概述

随着手机平台技术的不断发展，针对各类手机平台的恶意软件层出不穷，这些恶意软件已经威胁到了手机用户的隐私及财产安全。近年来，手机恶意软件主要以手机病毒、手机木马等形式存在于手机平台中，2009 年手机平台上开始出现与计算机平台上类似的僵尸网络。

传统的僵尸网络指的是攻击者利用互联网建立的可以集中控制的计算集群[1]。攻击者利用僵尸网络进行分布式拒绝服务攻击、发送垃圾邮件等恶意行为[2-4]。手机僵尸网络是僵尸网络在手机平台上的新发展，指的是攻击者通过手机僵尸程序建立的可控手机群体。与计算机平台上的僵尸网络类似，通过手机僵尸网络攻击者可以进行手机短信洪流攻击、发送垃圾邮件、订购高额 SP 服务等有害行为。这些行为极大地威胁着手机用户的隐私及财产安全。

目前已发现了若干手机平台上的僵尸网络。SYMBOS_YXES.B 于 2009 年 7 月被发现，该软件在感染用户手机后会搜集用户的个人资料、手机信息、网络信息等，并将这些信息上传到指定的服务器。此外，它还会发送大量的垃圾短信给被感染用户的联系人，短信内容由控制者的服务器提供。Ikee.B[5]出现于 2009 年 11 月，针对被破解的 iphone 手机。该软件感染用户后会搜集手机中与经济有关的敏感信息并上传到指定服务器，且能够通过该服务器获取命令并执行。

随着 Android 系统的推出及发展，使用 Android 系统手机的用户日益增多。由于 Android 系统的开放性，其安全问题一直是人们关心的重点。目前，Android 平台上已经出现了大量的手机恶意软件，其中一些已经带有手机僵尸网络的特征。文献[6]分析了手机僵尸网络的发展前景，并认为 Android 系统极有可能成为手机僵尸网络的新目标。

为了对抗僵尸网络，仅仅研究如何检测和防御已有的僵尸网络是不够的，还需要从攻击者的角度出发去研究可能发展出来的新型的僵尸网络。在针对 PC 平台僵尸网络的研究中已经有了相关的研究成果，如文献[7]提出了一种新的混合型 P2P 僵尸网络，文献[8]提出了一种高鲁棒性的新型 P2P 僵尸网络。本文构造了一种基于 Android 系统的手机僵尸网络，提出一种基于图片服务器及微博服务器的命令控制信道。

2 命令控制信道

与病毒、木马相比，僵尸网络的最大不同在于其存在一个或多个命令控制服务器。这些命令控制服务器往往是互联网上的公共服务器。命令控制服务器用于接收攻击者发布的命令并将这些命令下发给僵尸程序。命令控制服务器是整个僵尸网络中最薄弱的环节，若防御者切断了命令控制服务器，则控制者将失去对整个僵尸网络的控制。因此，对命令控制信道的研究有助于更好地检测、阻断僵尸网络。

对手机僵尸网络而言，必须存在适合其特点的命令控制信道。需要从控制者的角度出发构造一种适合手机平台的控制命令信道。对于控制者而言，可用的命令控制信道需要满足以下 3 种要求：

基金项目：国家“863”计划基金资助项目(2007AA010501)

作者简介：刘潇逸(1987－)，男，硕士研究生，主研方向：网络安全，僵尸网络；崔 翔，博士；郑东华、李 善，学士

收稿日期：2011-07-11 **E-mail：**liuxiaoy135@gmail.com

(1)控制者可以容易地掌握僵尸网络中每一台手机的状态及信息。

(2)控制者可以容易地发布命令。

(3)命令控制信道不容易被防御者切断。

目前，研究者们已经对手机僵尸网络的命令控制信道进行了相关研究。文献[9]提出了基于短消息服务(Short Message Service, SMS)的命令控制方式，通过手机的短信功能实现控制者对僵尸手机的控制，但这种方式没有考虑到僵尸手机发送短信时产生的费用问题，当僵尸手机发送大量短信用于命令控制时，手机用户很容易察觉异常的费用支出，进而有可能发现僵尸程序的存在并将其删除。文献[10]提出并讨论了基于蓝牙的命令控制方式，而蓝牙的最大缺点在于其发送接收距离很短，普通的蓝牙发送接收距离仅 10 m。由于这种局限性导致蓝牙很难作为手机僵尸网络的命令控制信道。

由于 Android 系统十分强调网络服务，运行 Android 系统的手机都有完善的上网功能，因此本文考虑利用手机的互联网功能构造命令控制信道。相比于短信服务和蓝牙，利用互联网实现命令控制信道使得手机僵尸网络的控制方式更加类似于计算机上的僵尸网络，并且互联网上的资源更加丰富，有助于设计适合手机的命令控制信道。本文使用互联网上的图片服务器及微博服务器构建了一种适合手机僵尸网络的命令控制信道。

2.1 命令图片的创建

为了利用图片服务器进行命令发布，控制者需要将命令与图片文件结合起来。本文采用的方法是将命令字节流写入到图片文件字节流中，僵尸程序获取到图片后再从图片字节流中取出命令。命令嵌入的效果如图 1 所示。其中，图 1(a)为嵌入命令前的图片，大小约为 2.32 KB，图 1(b)为嵌入命令后的图片，大小约为 2.47 KB，可以看到 2 张图片几乎看不出差别。

(a)加密前 (b)加密后

图 1 图片加密前后效果示意图

2.2 命令控制信道的构造

完成命令图片的创建后，本文利用图片服务器及微博服务器构造了手机僵尸网络的命令控制信道，如图 2 所示。

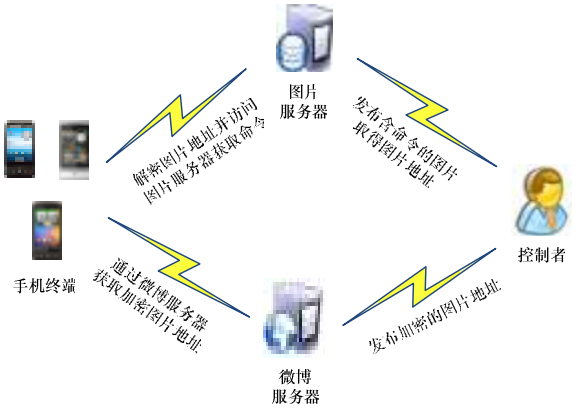

图 2 命令控制信道

命令控制流程如下：

(1)控制者将加入命令的图片发布到图片服务器并获取图片地址。

(2)控制者通过微博发布图片地址。

(3)僵尸手机每隔一段时间访问微博，尝试获取加密的图片地址。

(4)僵尸手机在成功获取图片地址后访问图片服务器并下载图片，获取并执行命令。

目前互联网上的免费图片服务器都存在一个特点，即当图片上传后服务器会生成一个随机的字符串作为图片名，并且该字符串将包含在图片地址中。由于这样会使得图片地址无法在发布前获得，控制者需要寻找另一种途径解决地址不可控问题。而对于微博服务器而言，当用户申请一个微博账号后，微博域名直接包含该账号名。控制者就可以通过微博域名的可控性解决图片地址不可控的问题。

3 僵尸手机状态回收

作为手机僵尸网络的控制者，必须能够掌握僵尸网络中每一部手机的状态。为此，需要寻找一种适合于手机平台的状态回收方式。

Android 系统提供了大量用于 HTTP 访问的系统函数，利用这些函数可以方便地进行 HTTP 访问，又因为互联网中有很多网站提供了免费个人服务器申请的功能，可很方便地获得用于接收僵尸手机状态的服务器。本文通过 HTTP 访问形式将手机的 IMEI(International Mobile Equipment Identity)号、手机号等信息发送给指定的服务器，以达到回收僵尸手机状态的目的。在回收的信息中，IMEI 是国际移动装备辨识码，每一台手机都拥有一个全球唯一的 IMEI 号。控制者可以通过 IMEI 号码标示僵尸网络中的每一台手机。

当通过 HTTP 访问无法回收僵尸手机状态时(如申请的服务器被撤销等情况)，本文通过邮件的方式回收手机状态。Android 系统下的可运行程序支持 Java 语言编写，本文利用 Java 提供的 Javamail 函数包实现僵尸程序的邮件接收及发送功能，通过邮件将手机状态发送到指定的邮箱中。目前，大多数门户网站均提供了免费邮箱，控制者只需要申请多个免费邮箱即可实现僵尸手机的状态回收。

4 手机僵尸程序恶意行为

文献[11]分析了目前手机恶意软件的主要行为，包括恶意扣费、系统破坏、隐私窃取等。手机僵尸程序也会拥有这些功能，并且由于可以被控制者集中控制，僵尸手机给用户造成的损失会比传统的手机病毒更严重。由于手机平台的特殊性，手机僵尸程序会拥有与计算机上的僵尸程序不同的功能。出于研究目的，本文为实现的僵尸程序设计了以下几种行为：搜集手机中的通讯录，获取手机中的短信内容，发送垃圾邮件，发送指定短信，进行短信洪流攻击等。而实际的手机僵尸网络必然会拥有订购高额服务等损害手机用户经济利益的行为。

通常普通用户的手机中都保存了大量的联系人信息，手机僵尸程序获取这些信息后再发送伪造的短信，短信中可以包含僵尸程序的下载地址以实现自我传播，也可以包含有害的网络链接，通常是高额 SP 服务的订购链接。若接收者点击了这些恶意链接则会造成大量的经济损失。

手机僵尸网络发送垃圾邮件的功能与计算机上的僵尸网络类似，即对邮件服务器进行分布式拒绝服务攻击。短信洪流攻击则是手机平台上特有的僵尸程序行为，与发送垃圾邮

件类似，攻击者利用控制的僵尸手机在特定时间向某一号码的手机发送大量垃圾短信，造成目标手机软件或硬件损坏。

5 手机僵尸网络的防劫持策略

在僵尸网络中，命令控制服务器是最薄弱的一个环节。僵尸网络的控制者必须加强对命令控制服务器的保护，避免因防御者切断命令控制服务器而使得整个僵尸网络瘫痪。

Android 系统中运行的程序主要由 Java 语言实现，Java 语言实现的程序容易被逆向破解，如防御者将僵尸程序破解，获得访问的微博域名则可以对其修改并劫持整个僵尸网络。因此，需要加入防劫持手段以保证僵尸网络的稳定可控。

5.1 多服务器策略

控制者可以使用多个图片服务器及微博服务器。在命令控制信道的构造过程中，本文选取了若干个国内外稳定且可访问的图片服务器及微博服务器，通过图片及微博服务器数量上的增加来保证僵尸网络不会因为其中某个或某些服务器的关闭而瘫痪。

5.2 微博域名 Flux

域名 Flux 技术是一种新兴的僵尸网络防劫持技术[12]。僵尸程序在运行过程中会生成一个随机域名列表，该列表对于控制者而言是可知的，并且会根据控制者实现设定的参数每隔一段时间改变一次。在每次尝试获取控制者命令时，僵尸程序会依次访问列表中的域名，直到访问到正确的域名，如果没有正确的域名则在遍历一次列表后结束访问，并根据控制者设定的时间间隔休眠一段时间再重新进行访问。控制者在需要发布命令时选择列表中的某个域名进行注册即可，而防御者很难通过关闭域名来切断控制者的命令控制信道。

本文在僵尸程序的编写中加入了微博域名 Flux 技术，用年粒度、月粒度、日粒度 3 种粒度做参数让僵尸程序生成多个随机的微博域名，其中，年粒度下的域名每一年更换一次，月粒度下的域名每个月更换一次，日粒度下的域名每天更换一次。僵尸程序每次进行服务器访问时以年粒度、月粒度、日粒度的顺序进行访问，直到访问到正确的微博地址。在发布命令时控制者可根据需要选择某种粒度下的某个域名进行注册。即使该域名被防御者关闭，控制者只需要重新根据列表注册一个域名即可恢复对僵尸网络的控制。

5.3 身份认证系统

假设防御者获得了僵尸程序，并对其网络访问进行监控，则有可能获得随机域名列表，进而找到控制者使用过的域名。由于微博发布后在网络上是公开的，防御者在找到控制者使用过的微博后极有可以发现真实的图片地址，获取图片，进而伪装成僵尸网络的控制者，劫持僵尸网络。为了防止这种情况的出现，控制者必须在命令发布以及接收的过程中加入身份认证系统，以保证只有自己发布的命令才能被僵尸程序执行。

为了达到身份认证的目的，控制者在发布命令时引入 RSA 签名机制[13]，对命令本身以及图片地址做签名，僵尸程序在获取命令时会先对签名进行验证，只有当验证成功时，僵尸程序才认为是控制者发布的命令，再获取并执行命令。RSA 签名密钥包含 2 个部分，即公钥 K_{Pub} 和私钥 K_{Pri}。K_{Pri} 由控制者拥有，用于对命令和图片地址做签名，K_{Pub} 硬编码在僵尸程序中，用于对签名的命令和图片地址做认证。对于防御者而言，即使掌握了控制者使用的微博，甚至获取到僵尸程序，但由于无法获取 K_{Pri}，就无法控制者的签名，也就无法劫持整个僵尸网络。

6 手机僵尸网络的流量控制

与计算机网络包月付费不同，手机网络目前主要以包流量形式为主，控制者必须考虑僵尸程序获取并执行命令时产生的流量问题，若僵尸程序在访问微博及图片服务器的流量过多，用户极易发现异常的流量费用，进而可能发现僵尸程序并将其删除。因此，控制者需要控制僵尸程序的网络访问流量，降低用户的费用消耗，减少僵尸程序被发现的可能。本文从 2 个方面对僵尸程序网络访问部分进行优化：(1)设置合适的访问间隔；(2)减少每次访问产生的流量。

6.1 访问间隔设置

由于采用了微博域名 Flux，僵尸程序每次会访问多个微博，如果访问的间隔过短，僵尸程序会因为频繁链接网络消耗大量流量，而如果访问的间隔过长，又会导致僵尸程序不能及时获取新命令，影响命令执行的时效性。本文将访问间隔调整到一个合适的值，通常为 1 h 内访问 1 次~2 次，以保证僵尸程序既能较快获得新命令，又不会因为多次访问产生过多的流量消耗。

6.2 访问流量控制

本文通过 3 种途径减少访问时产生的网络流量：

(1)通过 RSS 订阅访问微博；

(2)压缩图片地址及图片大小；

(3)使用 GZIP 压缩传输。

RSS 是在线共享内容的一种简易方式。使用 RSS 订阅能更快速获取信息，网站提供 RSS 输出，有利于让用户获取网站内容的最新更新。对于手机僵尸网络而言，RSS 最大的优点是其消耗的流量很少，因为 RSS 的页面把与浏览无关的广告、图标、各种连接等都过滤掉，极大地降低了访问产生的流量。而目前的微博大部分都提供了 RSS 订阅功能，僵尸程序只需要访问相应微博的 RSS 订阅页面即可获取图片地址。本文选取了国内较为知名的嘀咕微博，随机访问了其中若干用户的微博主页及其对应的 RSS 订阅页面，对其页面大小进行了比较，比较结果如表 1 所示，可以看出，访问 RSS 订阅页面可以极大地减少访问流量。

表 1 微博页面与 RSS 页面大小比较 KB

用户名	微博页面大小	RSS 订阅页面大小
Lan617	72.8	18.6
nbgirl	67.9	22.6
dandanai	67.4	17.0

由于微博每次发布有字数限制，国内微博限制每次最多发送 140 个汉字，因此如果直接对图片地址进行签名并发布，需要至少发送 3 条微博才能完成一次命令发布，而利用域名压缩技术则发送 2 条微博即可完成一次命令发布。又因为图片只是加载命令的手段，图片本身的大小并不会影响命令的嵌入，所以笔者尽量选择体积小的图片，减少僵尸程序每次下载图片产生的网络流量。

目前大多数网站均提供了 GZIP 压缩传输功能，当用户来访问网站时，网站服务器将网页内容压缩后传输给用户，GZIP 对纯文本内容可压缩到原大小的 40%。因为 RSS 订阅页面为纯文本页面，所以使用 GZIP 压缩传输能够更进一步减少僵尸程序的访问流量。

6.3 访问流量测试

为了更深入地掌握僵尸程序每次获取命令过程中产生的流量情况，本文对僵尸程序访问微博及图片服务器时产生的流量数据进行了统计，分 3 种情况统计了僵尸程序在访问不

存在的微博域名、访问存在的微博域名以及下载命令图片时产生的流量。表 2 显示了 3 种情况下的流量统计。

表 2 僵尸程序网络访问流量统计 Byte

网络访问	上行流量	下行流量	总流量
访问存在的微博	504	1 438	1 942
访问不存在的微博	504	676	1 180
下载图片	1 299	3 885	5 184

具体测试如下：

(1)每次访问 1 个不存在的微博域名，多次测试后求平均值。测试结果显示，访问 1 个不存在的微博产生下行流量 676 Byte，上行流量 504 Byte，共产生流量 1 180 Byte。

(2)访问一个正确的微博，微博中发布了一个命令图片的地址。仅测试访问微博产生的流量，多次测试后得到平均值得到每次访问产生下行流量 1 438 Byte，上行流量 504 Byte，共产生流量 1 942 Byte。

(3)访问一个正确的微博，仅统计下载图片时产生的流量，使用的图片大小为 2 531 Byte。多次测试后的平均值为：下载一次图片产生下行流量 3 885 Byte，上行流量 1 299 Byte，共产生流量 5 184 Byte。

以每次生成 30 个随机域名来计算，在没有命令即 30 个域名都不存在的情况下，每次共需要约 33 KB 的流量。若一个用户每月包流量 30 MB，则僵尸程序可以每 1 h 进行一次访问，若用户每月包的流量更多则僵尸程序的访问间隔可以进一步缩短。由此可以看出，使用 RSS 页面以及 GZIP 压缩较好地解决了僵尸程序在尝试获取命令过程中产生的网络流量消耗问题。

7 手机僵尸网络防御

僵尸网络中最薄弱的环节就是命令控制服务器，如果能够找到控制者使用的命令控制服务器，就可以将其关闭，切断整个僵尸网络，而且掌握命令控制服务器，可以了解僵尸网络的规模以及其行为特征。

蜜罐技术是一种有效的检测僵尸网络的技术，防御者让蜜罐手机感染僵尸网络程序，使得蜜罐手机进入僵尸网络内部。如果控制者无法检测出僵尸网络中的蜜罐手机，防御者就可以通过蜜罐手机观察僵尸程序的行为。蜜罐手机进入僵尸网络后必然会与命令控制服务器进行交互。通过对蜜罐手机进行监测，防御者就有可能找到控制者使用的命令控制服务器，并对其进行监控。通过蜜罐手机防御者还有可能获得控制者发布的命令，如果命令中包含了控制者将要攻击的对象，防御者就可以提前进行防御。此外，防御者可以利用蜜罐手机得到僵尸程序访问的域名列表，进而监控列表，注册列表中域名的人很有可能就是僵尸网络的控制者。

在得到僵尸程序的样本后还可以对其进行反编译以寻找到有用的信息。防御者在获得僵尸程序样本后可对其进行反编译，就有可能找到负责域名列表生成的代码段。得到这些代码段就意味着防御者可以预知僵尸程序将来要访问的所有域名，这样就扩大了可监控的域名范围，更有效地切断僵尸网络的命令控制信道。

目前的手机恶意软件主要通过社会工程学方法进行传播，例如通过带有恶意链接的短信，或是将带有恶意代码的软件发布在网上供人下载。因此，作为防御者可以通过设计一种检测系统来监测用户短信中出现的链接，并获取链接中的程序。一旦发现程序存在恶意行为防御者就能够提醒用户不要点击相关链接。此外，防御者需要重视手机软件的发布管理，加强对软件的功能检测，减少恶意软件发布给用户下载的可能。

8 结束语

随着移动平台的发展，手机安全问题日益严重，手机病毒、木马层出不穷。手机平台上也出现了类似计算机平台的僵尸网络。Android 系统由于其开放性成为了病毒制造者们关注的焦点。目前 Android 系统上已经出现了多个病毒程序，其中一些病毒已经出现了僵尸网络的特征。为了更好地面对未来手机平台的僵尸网络。本文通过对 Android 系统上僵尸网络的构造，揭示了手机僵尸网络的可行性以及危害性，设计了一种适用于手机僵尸网络的命令控制信道，并对手机僵尸网络的防劫持技术、流量控制技术及防御策略进行了讨论。下一步将对手机僵尸程序的传播方式进行分析，研究 Android 系统下僵尸程序的植入及免杀技术。

参考文献

[1] 杜跃进, 崔 翔. 僵尸网络及其启发[J]. 中国数据通信, 2005, 7(5): 9-13.

[2] Freiling F, Holz T, Wicherski G. Botnet Tracking: Exploring a Root-cause Methodology to Prevent Distributed Denial-of-service Attacks[C]//Proc. of the 10th European Symposium on Research in Computer Security. Berlin, Germany: Springer, 2005.

[3] Dagon D, Zou C, Lee W. Modeling Botnet Propagation Using Time Zones[C]//Proc. of NDSS'06. Berkeley, USA: [s. n.], 2006.

[4] Ramachandran A, Feamster N, Dagon D. Revealing Botnet Membership Using DNSBL Counter-intelligence[C]//Proc. of the 2nd Conference on Steps to Reducing Unwanted Traffic on the Internet. Berkeley, USA: [s. n.], 2006.

[5] Porras P A, Saidi H, Yegneswaran V. An Analysis of the Ikee.B (Duh) iPhone[C]//Proc. of ICST'10. Berlin, Germany: Springer, 2010.

[6] Schmidt A D, Schmidt H G, Batyuk L, et al. Smartphone Malware Evolution Revisited: Android Next Target?[C]//Proc. of the 4th IEEE International Conference on Malicious and Unwanted Software. [S. l.]: IEEE Computer Society, 2009.

[7] Wang P, Sparks S, Zou C C. An Advanced Hybrid Peer-to-Peer Botnet[C]//Proc. of the 1st Conference on First Workshop on Hot Topics in Understanding Botnets. Berkeley, USA: [s. n.], 2007.

[8] 谢 静, 谭 良. 一种高鲁棒性的新型 P2P 僵尸网络[J]. 计算机工程, 2011, 37(7): 154-156.

[9] Zeng Yuanyuan, Hu Xin, Shin K G. Design of SMS Commanded and Controlled and P2P-structured Mobile Botnets[EB/OL]. [2011-03-20]. https://www.eecs.umich.edu/techreports/cse/2010/CSE-TR-562-10.pdf.

[10] Singh K, Sangal S, Jain N, et al. Evaluating Bluetooth as a Medium for Botnet Command and Control[C]//Proc. of DIMVA'10. Berlin, Germany: Springer, 2010.

[11] 北京网秦天下科技有限公司. 2010 年中国大陆地区手机安全报告[EB/OL]. [2011-03-20]. http://www.netqin.com/upLoad/File/baogao/2010anquanbaodao(1).pdf.

[12] Ollmann G. Botnet Communication Topologies[EB/OL]. [2011-03-20]. http://www.damballa.com/solutions/downloads.com.

[13] Rivest R L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-key Cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

编辑 顾姣健