一种基于 SMS 的移动僵尸网络的设计及分析

徐 建
(南京邮电大学 计算机学院,江苏 南京 210023)

摘 要:僵尸网络是计算机重要的安全威胁。随着智能手机的发展,这一安全威胁出现在智能手机上。现在手机中毒已成为普遍现象,在研究了手机传播病毒方式的基础上,对移动僵尸网络的传播、命令控制机制以及控制协议进行了深入研究,分别分析了结构化和非结构化的拓扑结构,用示例来描述如何将 SMS 信息的 C&C 通道与 P2P 的拓扑结构相结合,对基于 SMS 的移动僵尸网络进行设计和分析。对于移动僵尸网络这种新型的手机病毒攻击模式将会严重影响人们的生活,因此必须不断地研究、发现各种威胁手机的行为。

关键词:移动僵尸网络;命令控制;P2P;拓扑结构
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2016)01-0106-05
doi:10.3969/j.issn.1673-629X.2016.01.022

Design and Analysis of a SMS-based Mobile Botnet

XU Jian
(College of Computer Science, Nanjing University of Post and Telecommunications, Nanjing 210023, China)

Abstract: Botnet is an important threat on computer security. As the development of smart phones, the security threats appeared on the smart phones. Now mobile phone infected virus has become a common phenomenon. Based on the research of mobile phone virus spreading on the way, the spread, command and control mechanisms, and control protocol of mobile botnet are studied in-depth, respectively analyzing the topology of structured and unstructured. Use example to describe how to combine SMS C&C and P2P structure. Based on the SMS mobile botnet, carry on the design and analysis. For mobile botnet, a new type of virus attack mode for mobile phone, will seriously affect people's life, so the continuous study is done and the behavior of the various threats to mobile phones is found.

Key words: mobile botnet; C&C; P2P; topology

0 引 言

僵尸网络的建立和防御一直是很多研究人员关注的热点问题,它是网络中最严重的安全威胁之一。僵尸网络是攻击者所掌握的一种攻击平台,攻击者利用各种手段传播僵尸程序,将大量主机感染成僵尸机,并通过命令与控制信道操纵这些僵尸机,实施分布式拒绝服务攻击、垃圾邮件发送以及敏感信息窃取等恶意行为[1]。虽然它们在现实中没有造成大面积的爆发,但近年来攻击蜂窝网络设备的数量在不断增长并逐渐成熟。随着智能手机的发展,例如:Iphone、安装了安卓系统的手机等,它们下载和共享的第三方应用程序及用户生成的内容急剧增加,使得智能手机很容易受到各种类型恶意软件的破坏。大多数智能手机上都安装了具有多功能的操作系统,比如 Linux, Windows Mobile, IOS, Android 以及 Symbian OS 等。安装了系统的智能手机在运行环境中越来越近似于 PC 机,但安全保护却远远比不上 PC 机,这也诱导了犯罪。在安卓市场已有许多有关恶意应用程序的报道[2]。由于安卓平台的策略是要求开发者自己签署自己的应用程序,因此攻击者很容易将恶意软件放入市场中。而苹果应用商店控制它的应用就很严格,但不包含已“越狱”的苹果产品,它可以安装任何应用,并在后台运行进程。

现在科研人员针对传统僵尸网络的研究已比较全面,如僵尸网络威胁[3]、僵尸网络分类[4]、僵尸网络模型[5]、僵尸网络控制策略[6]和僵尸网络检测[7]等。然

收稿日期:2015-01-27 **修回日期**:2015-06-10 **网络出版时间**:2016-01-04
基金项目:国家自然科学基金资助项目(61202353);江苏省高校自然科学研究资助项目(12KJB520008);南京邮电大学实验室工作研究课题(2015XSG05)
作者简介:徐 建(1980-),男,硕士,工程师,研究方向为信息安全、人工智能。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160104.1453.002.html

而针对智能手机的移动僵尸网络的研究才刚起步,如基于 SMS 短信信道建立的移动僵尸网络[8]、基于蓝牙通信建立的移动僵尸网络[9]、基于无线网络的移动僵尸网络[10]等。

早期的僵尸网络主要是利用 IRC 协议、HTTP 协议来建立,比如 Rbot 和 Zeus[11]等,僵尸机与僵尸主控机之间主要是 C/S 结构。现在看来这种经典的结构存在两个致命的弱点:很容易产生单点失效的问题;僵尸主控机很容易被发现,而且一旦发现,整个网络都将瘫痪。

随着网络的不断发展,P2P 技术的出现,基于 P2P 技术的僵尸网络也应运而生。因此文中从 P2P 技术出发,比较了几种 P2P 的拓扑结构,建立基于 SMS 控制的移动僵尸网络模型。

1　移动僵尸网络的研究

主要是由攻击者通过感染大量的移动智能终端(多指手机),利用移动互联网平台搭建命令控制信道,进行远程控制使其进入特定受控状态的移动智能终端群,称之为移动僵尸网络,又名手机僵尸网络[12]。在移动互联网中,移动智能终端是主要的消息传输介质,版本多、操作系统多样、支持业务种类多,因此僵尸网络在移动互联网上的传播具有多样性并很难统一控制,安全事件的检测与追踪比互联网更加困难。由于移动网络升级很快,GSM、3G、LTE 的网络制式不仅在迅速升级,同时还存在着不同制式的网络并网的问题。因此,移动智能终端必须支持多种网络制式的协议。智能终端操作系统频繁更新,产品的硬件环境同样更新频繁。移动终端用户群具有业务迁移迅速和多变等特性。但这里所谈的移动智能终端主要是以智能手机为主,而智能手机的操作系统是以 Android 和 IOS 最常见。由于苹果公司的产品并没有完全开源,因此文中研究主要是基于 Android 系统。从传播、C&C 的通道、拓扑结构三个方面来研究移动僵尸网络。

1.1　移动僵尸网络的传播

移动僵尸网络传播的目的是为了不断增加感染手机的数量,构建更大的僵尸网络,而且所有的传播机制都是在用户不知情的情况下完成的,并带有一定的攻击性的行为。现在所使用的智能手机频繁访问互联网,成为恶意攻击的目标。因此垃圾邮件和 SMS/MMS 消息的恶意附件,或指向恶意网站的网址,可以方便地找到并进入手机的收件箱。用户有意无意会打开附件或点击这些网址下载恶意程序。攻击者侵入了用户的手机就可以获得大量的电话号码,而一般使用的电话号码与个人信息都是紧密相连的,这样将会泄露大量的个人信息。据 2013 年 6 月卡巴斯基实验室的最新报告显示,其“首次发现了黑客通过使用不同的移动恶意软件来创建僵尸网络并以此来传播恶意软件的案例”。该僵尸网络由 Obad. a 和 Opfake. a 程序搭配组成,用户一旦安装了该程序后将导致 Android 设备受感染并使得恶意软件得到大面积的传播。卡巴斯基称,Android 木马程序 Backdoor. AndroidOS. Obad. a 是恶意软件的罪魁祸首。一位名为 Roman Unuchek 的卡巴斯基实验室专家写道,Obad. a 采用了入侵 Android 常用的方式,如短消息服务(即短信)、垃圾信息、假冒 Google Play 商店,以及被黑掉的或不可信的 Android 软件下载站点等,其最新的伎俩则使得该木马比普通的 Android 木马更具传染性。在实际情况中,Obad. a 是与另一个手机木马 SMS. AndroidOS. Opfake. a 一起传播的。这个木马使用了入侵 Android 的常用方式并伪装为一个用户想要下载的应用程序。一旦用户被种下该木马病毒,Opfake. a 就会利用 Google 云消息服务(GCM)给用户发送一条短信,短信内容如下:彩信已发送成功,请点击 www. otkroi. com 下载。如果用户点击了这个链接,一个名为 mms. apk 的文件就会自动下载到用户的智能手机或平板电脑上,该文件中包含有 Opfake. a 程序。而后,用户如果选择运行这个应用程序,那么僵尸网络的命令和控制服务器就能够给该木马发送指令,向用户设备上的所有联系人发送以下消息:您有一条新彩信,请点击 http://otkroi. net/12 下载。一旦用户点击这个链接并下载彩信,那么 Obad. a 就会被自动加载到 mms. apk 或 mmska. apk 的文件名下。用户如果运行了这些程序,其就将成为 Obad. a 的一个传播网络。据 Unuchek 介绍,一家俄罗斯大型移动运营商的统计数据表明,“在短短 5 个小时内,就有 600 条带有 Trojan-SMS. AndroidOS. Opfake. a 木马的短消息被成功发送。多数情况下这些短消息都由受感染的移动设备发出,而此前黑客就曾利用短信网关做了几次类似的病毒传播。另一方面,目前只有少数设备受到 Opfake. a 的感染,Opfake. a 会通过发送链接让用户下载 Obad. a 程序,因此可以得出一个结论,即该恶意木马的创建者是通过租用部分移动僵尸网络来实现对恶意软件的传播。而这导致的最终结果,就是使得该僵尸网络能够迅速传播 Opfake. a 和 Obad. a 程序[13]。另一种传播方式可以利用蓝牙功能,移动手机用户通过蓝牙搜索配对附近的设备,在连接成功后传播恶意软件。还有可能通过与 PC 机连接感染恶意软件,在自己安装手机系统时被感染。恶意软件的传播是无孔不入的,但最主要的感染方式大都是通过系统的漏洞进行传播。

1.2　命令与控制

当前主要使用的僵尸网络命令与控制机制包括:

基于 IRC 协议的命令与控制机制、基于 HTTP 协议的命令与控制机制,以及基于 P2P 协议的命令与控制机制[14]。

1.2.1 基于 IRC 协议的命令与控制机制

IRC 协议是早期因特网广泛使用的一种基于 C/S 模式的实时网络聊天协议,用户通过客户端连接到服务器上,服务器可以连接多个客户端,所有客户端通过服务器互相连接构成庞大的 IRC 聊天网络,可以将用户的消息通过聊天网络发送到目标用户或用户群。用户可以选择加入自己感兴趣的频道,在同一频道中,用户可以向所有其他用户发送消息,也可以单独给某一个用户发送。攻击者正是利用了 IRC 协议的简单、低延迟、匿名的实时通信方式,设计了基于 IRC 协议的命令与控制机制。攻击者可以通过 IRC 服务器向僵尸机发送各种命令,其中比较经典的两条命令是 advscan lsass 20050-r-s 和 http. update http:/server/rBot. exe c:\rBot. exe 1。主要目的是利用 lsass 漏洞,开始随机扫描;后一个是下载 rBot. exe 文件到 C 盘并执行。

1.2.2 基于 HTTP 协议的命令与控制机制

基于 HTTP 协议的命令与控制机制是近年来另外一种流行的基于 C/S 架构的僵尸网络控制机制。攻击者通过 HTTP 网站,发布命令脚本,僵尸机通过 HTTP 协议访问该网站的网页,然后根据该脚本进行相应的操作。它的使用具有两个方面的优势:首先,隐蔽性好,在大量的互联网 Web 流量中,它的活动很难被检测;其次,HTTP 协议的控制和通信流量能轻易地穿越防火墙,而 IRC 协议所使用的端口就比较容易被过滤。这种方式也有它的缺点,只有当僵尸机访问服务器网页时,才能获得控制者发布的命令,因此在实时控制方面比较弱。

目前,比较典型的 HTTP 协议构建命令与控制机制的僵尸程序有 Bobax、Rustock、Clickbot 等。如 Bobax 僵尸程序,被植入僵尸程序的主机会伪装成浏览器来访问指定服务器上的某个网页,类似于“http://hostname/reg? u=[8-digit host id]&v=114”的一个 URL,如果连接成功,则僵尸网络控制器将反馈这个请求,并在返回内容中包含攻击者发出的控制命令,Bobax 僵尸程序就会从返回信息中解析出命令并执行,Bobax 僵尸程序接收的命令包括:下载更新程序(upd)、执行程序(exe)、扫描主机(scn)、停止扩散扫描(scs)、发送垃圾邮件(prj)、报告网络连接速度(spd)等。

1.2.3 基于 P2P 协议的命令与控制机制

基于 IRC 协议和 HTTP 协议的命令与控制机制都是建立在 C/S 架构下的,都是通过中心服务器来控制的,这样的结构一旦防御者获得僵尸程序,它们就能很容易地找到中心服务器的位置,将给整个僵尸网络带来毁灭性的破坏。为了增加僵尸网络的韧性和隐蔽性,许多僵尸程序采用了 P2P 协议构建其命令与控制机制。在基于 P2P 协议的僵尸网络中,没有中心控制点,攻击者只需向一台僵尸机发布命令,在僵尸网络中的机器将会相互发布并执行。常见的有 Sinit、Phatbot、SpamThru、Nugeche、Peacomm 等。这种命令与控制机制即使有部分僵尸机被破坏,也不会对整个网络造成严重的影响,因此对于建立的移动僵尸网络而言,更需要采用 P2P 协议的命令控制机制。由此,文中提出了利用 SMS 通信与 P2P 技术相结合的移动僵尸网络模型。

2 基于 SMS 控制的移动僵尸网络模型

2.1 SMS 命令控制机制

SMS(短信服务)是一种存储、转发服务。也就是说,发送人始终是通过 SMSC(短信服务中心)转发到接收人的。如果接收人处于未连接状态(可能电话已关闭),则信息将暂存在 SMSC,当接收人再次连接时,再次发送。文中就是利用 SMS 作为命令控制信道建立移动僵尸网络,在感染的僵尸机和僵尸主机之间通过 SMS 进行通信。在 PC 机中,僵尸网络的 C&C 是基于 IP 来传送,而智能手机与之不同,它很难建立和维护稳定的基于 IP 的连接。主要原因是它一直处于移动的状态,而且建立一个私有的 IP 地址连接到网络比较困难。文中选择短信作为 C&C 通道有它的优势。首先,SMS 文本消息在所有应用程序中是应用最广泛的,有超过 80% 的手机用户发送和接收短信,只要手机一打开,这个应用就会处于活跃状态。其次,如果手机关机或者在信号很弱的地区,SMS 通信信息将会被存储在服务中心,一旦开机或者信号强烈时,还可以接收到此信息,因此很容易实现离线的僵尸机。第三,一些恶意的内容很容易隐藏在 SMS 信息里。在日常生活中,绝大多数的手机都会收到垃圾信息,也许这些信息根本就无关紧要,但在收到信息的同时,控制僵尸机的命令已经到达了你的手机,最理想的状态就是在用户不知情的情况下,让手机安装上设定好的僵尸代码并执行命令。当前有许多种方式来发送和接收免费的短信,因此在不影响短信息的情况下,将命令编码写进短信息里,就可以轻易地在手机后台下载安装控制命令。为了能更好地在手机之间进行控制和通信,每个受控的手机上都会有一个 8 位的密码,只有通过了密码认证的被控手机才能与其他被控手机进行通信。当手机接收到包含有 C&C 信息的短信时,它将会搜索其密码和嵌入在信息里的命令。如果发现存在,手机将立即执行此命令。

在移动僵尸网络中,由僵尸主控机分配到每个不

同功能的子僵尸网络的密码是不相同的。例如,一个子僵尸网络负责发送垃圾短信,而另一个子僵尸网络专门窃取个人资料,并传递到恶意服务器。在同一个子僵尸网络的所有僵尸机共享相同的密码,这样子僵尸网络中的僵尸机,以及与僵尸主控机的沟通都很方便。当然,若给每个僵尸机分配不同的密码会更安全,但是这样就会增加通信交换的开销,更容易被暴露。在每个 SMS 通信消息中不仅需要包含一个密码,而且在编码中的命令也不能让用户识别出来。在实际当中,相比安卓系统,其他移动平台大都是闭源的,限制也很多,在用户不知情的情况下,禁止发送和接收 SMS 信息。即使主要针对安卓系统,也需要对 C&C 信息进行隐藏,要不很容易被防御者所捕获和操纵。为了逃避防御者的检测,要将命令嵌入在 SMS 信息里,要让用户看上去更像垃圾信息,这样可以保证能安全地传递 C&C。文献[15]中指出,移动运营商不能简单地阻止违法短信,因为发送方支付了信息费用,当这些信息不包含垃圾信息的文件时,运营商担心永久删除了合法的信息。即使运营商过滤了垃圾短信或类似于电子邮件过滤,转储到垃圾邮件文件夹。垃圾短信通过目录仍然可以到达目标手机,再加上用户会忽视垃圾邮件,这样更有助于 C&C 的隐藏。

由于每个 SMS 消息只能包含有 160 个字符,因此隐藏在 SMS 信息里的 C&C 命令一定要简短。比如,“FIND_NODE”指示僵尸机返回特定节点的电话号码;“SEND_SYSINFO”要求僵尸机返回系统信息。为了隐藏消息,每个命令都被映射到一个垃圾邮件模板。额外的信息,如电话号码和前面提到的密码模板变量都是 64 位编码的[16]。如图 1 所示,有两个伪装的短信。

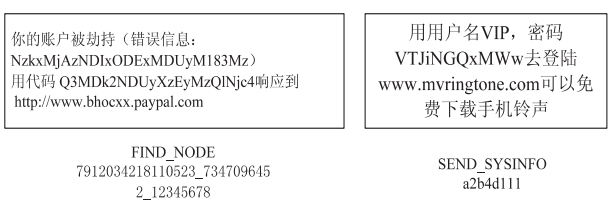

图 1　伪装的 SMS 信息

第一个是“FIND_NODE”信息(146 个字符),密码是 12345678,需要收件人来定位 ID 是 7912034218110523 的僵尸机,并将结果返回给号码为(743)7096452 的僵尸机。NzkxMjAzNDIxODExMDUyM183Mz 和 Q3MDk2NDUyXzEyMzQlNjc4,这两个随机字符串合在一起是 64 位的编码,是由 7912034218110523_7347096452_12345678 加密形成。整个字符串分为两个部分,一部分伪装成错误信息,另一部分当作类似于垃圾信息的代码。第二个例子是“SEND_SYSINFO”信息(98 个字符),密码是 a2b4d111。这个模板与“FIND_NODE”不同。密码也是 64 位的编码,密码显示在伪装的信息里。每个僵尸机都为解码信息保存着命令模板映射列表。由于在僵尸网络中有数以万计的命令,因此这样的列表不会太长。为了增加检测难度,一个命令消息可以对应不同的垃圾信息模板,而且模板还可以定期更新。显然,一个命令以及相关信息可以很容易地嵌入到 SMS 信息中,显示给手机用户的是他们熟悉的垃圾信息,因此他们很可能忽视这样的信息,或者打开并浏览。如果用户选择删除这些信息,对整个僵尸网络也没有任何影响,因为命令在信息接收的时候已经执行了。如果没有监视手机的行为或可逆工程,防御者也很难计算出垃圾信息模板和命令之间的映射关系。

用手机发送 SMS 信息,不仅可以在蜂窝网络实现,还可以通过互联网来发送。通过互联网发送信息可以更好地隐瞒自己的身份,降低成本。因此在移动僵尸网络中,利用短信作为 C&C 是可行的。

2.2　移动僵尸网络的拓扑结构

前面主要描述了利用 SMS 来建立 C&C 的通道,还需要创建僵尸主控机与僵尸机之间的组织结构。在研究现有的 P2P 拓扑结构的基础上,稍作修改来满足移动僵尸网络的构建。它与 PC 机的僵尸网络类似,无论是传统的集中方法,还是在分散的 P2P 方法,都可以建立移动僵尸网络。在集中式的方法中,僵尸主控机直接将可执行的代码硬编码到每个僵尸机,直接受它的控制。当一个手机被感染成僵尸机时,就可以通过那些硬编码接收和等待僵尸主控机的命令。像这种集中式的移动僵尸网络很容易实现,也很容易被破坏,一旦防御者获得这个代码,就可以追踪到僵尸主控机,并禁用僵尸网络。因此为了提高移动僵尸网络的鲁棒性,采用了 P2P 的结构。目前 P2P 的网络结构可以分为四类:中心化拓扑结构、全分布式非结构化拓扑结构、全分布式结构化拓扑结构、半分布式拓扑结构。

第一类,中心化拓扑结构维护简单,发现资源效率高,但是它依赖中心化的目录系统,与传统的 C/S 结构类似,很容易造成单点失效。使用此种结构比较经典的是 Napster 软件。

第二类,全分布式非结构化拓扑结构是在重叠网络(Overlay Network)采用随机图的组织方式,节点度数服从 Power-law 规律(幂次法则),能够很快发现目的节点,容错能力强,具有较好的可用性。一个典型的实现是 Gnutella,它不是指一个软件,而是遵守 Gnutella 协议的网络和软件的统称。

第三类,全分布式结构化拓扑结构主要是采用分布式散列表(Distributed Hash Table,DHT)技术来组织网络中的节点。DHT 能够自适应节点的动态加入/退出,具有比较好的鲁棒性和可扩展性。只要在网络中

存在的节点,DHT 都可以精确地发现它。

第四类,半分布式拓扑结构也被一些学者称为混杂模式。它吸收了以上一些结构的优点,选择性能较高的节点作为超级节点,在各超级节点上存储系统中其他部分节点的信息,发现算法只在超级节点之间转发,超级节点再将查询请求转发到适当的叶子节点,这种转发方式就是一种层次结构,是建立在超级节点与普通节点之间构成的若干层次。

为了能适应移动僵尸网络的需要,可以将结构化的和非结构化的 P2P 结构进行修改。由于智能手机与电脑的差异,而且手机采用的是短信 C&C 通道,因此对全分布式结构化拓扑结构的 Kademlia 进行一些修改。

首先不使用 PING 消息来查询节点,因为短信的传输是肯定可以达到的,而且还可以减少 C&C 的流量,从而减少被手机用户和防御者发现;其次,节点 ID 是由散列电话号码构成的,而不是随机生成的;最后使用公钥算法来确保命令的内容。在发布命令时,僵尸主控机给命令附加一个数字签名,这个签名是僵尸主控机的私钥,它是命令的散列值,其相应的公钥被硬编码到每个僵尸机的二进制码中,这样僵尸机在存储命令时可以检查是否真的来自于僵尸主控机。而对于非结构化拓扑结构,为了减少短信的信息量,去除了单跳重复的方法。那是由于在短时间里频繁接收/发送大量的短信,很容易被用户发现。

2.3 SMS 的 C&C 通道与 P2P 拓扑结构的结合

如何能够清楚地认识到利用 SMS 传播 C&C 消息与结构化的 P2P 拓扑结构的结合来适应移动僵尸网络。美国密歇根大学的 Zeng 博士用了一个简单的例子来说明命令发布和搜索的过程[16]。

如图 2 所示,为了方便演示,节点 ID 和数据项的键长都是四位的,发送的 SMS 信息没有伪装成垃圾邮件。在图中,节点 1111 要输入键 0111。在 Kademlia 中,数据项存储的节点 ID 接近于数据项的键。为了定位这些节点,节点 1111 先发送 SMS 信息到节点,这些节点在它的硬编码节点列表上;这些节点帮助获取在节点列表附近的节点。这个过程一直继续,直到没有节点能找到(这个过程图中省略了)。最后,节点 1111 找到了最接近的节点 0110(0110 ⊕ 0111 = 0001),接着发布包含命令键(0111)的消息,将加密命令(XXXX)与密码(8888)一起发送到节点 0110。验证了预定义的密码和命令之后,节点 0110 存储这些信息,以便以后任何节点需要请求与 0111 键相关的命令,它能够返回这些命令。至于搜索过程,它类似于信息发布过程的描述。节点 0000 查找与 0111 键相关的命令,一定会找到一个节点,它的 ID 接近这个键。节点 0000 首先查找 0010 节点;节点 0010 指向节点 0100;节点 0100 提供了最近的节点 0110。节点 0000 联系节点 0110 去请求命令。

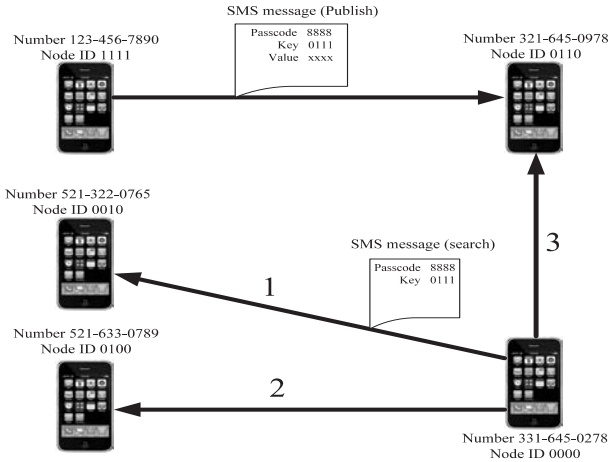

图 2 发布与搜索

从这个例子可以很直观地发现 SMS 的 C&C 通道与 P2P 拓扑结构的结合,以及在移动僵尸网络中的应用。但这只是冰山一角,还有许多更深层次的应用有待研究。

3 结束语

随着智能手机的飞速发展,在潜在利益的驱使下,它们成为僵尸网络攻击的目标。文中提出了一种 SMS 信息的 C&C 通道与 P2P 拓扑结构相结合的移动僵尸网络模型。攻击者利用手机短信传播 C&C 信息,以 P2P 结构作为它的拓扑结构。分别对结构化和非结构化的拓扑结构进行了分析,发现修改的 Kademlia 很适合在移动僵尸网络中应用。今后对移动僵尸网络的研究要更加详细和具体,不仅是如何建立,还要研究如何检测、防御和破坏。

参考文献:

[1] 王海龙,唐 勇,龚正虎. 僵尸网络命令与控制信道的特征提取模型研究[J]. 计算机工程与科学,2013,35(2):62-67.

[2] Google yanks over 50 infected apps from android market[EB/OL]. 2011-03-02. http://www.computerworld.com/article/2506378/security0/google-yanks-over-50-infected-apps-from-android-market.html.

[3] Geer D. Malicious bots threaten network security[J]. Computer,2005,38(1):18-20.

[4] 方滨兴,崔 翔,王 威. 僵尸网络综述[J]. 计算机研究与发展,2011,48(8):1315-1331.

[5] Song Lipeng,Jin Zhen,Sun Guiquan. Modeling and analyzing of botnet interactions[J]. Physica A,2011,390(2):347-358.

(下转第 123 页)

4　结束语

选取 Haar 小波基对测井曲线数据进行小波分解,对测井曲线噪声进行去除时,既能够很好地保持原始测井曲线的信息,又提高了测井曲线的空间分辨率,而且还使得测井曲线的信噪比达到了最佳值,与此同时对测井曲线的高频信息进行了改善。经过 Haar 小波去噪处理过的测井曲线更有利于人眼的观察,其细节信息更加丰富、清晰,畸变也很小。采用分步识别的方法解决套前自然伽马曲线与套后自然伽马曲线在形态上的相似性识别不准确的问题,为进一步进行完井校深工作提供了完备的理论与实践基础。

参考文献:

[1] 马世忠,黄孝特,张太斌. 定量自动识别测井微相的数学方法[J]. 石油地球物理勘探,2000,35(5):582-586.

[2] 刘红歧,陈　平,夏宏泉. 测井沉积微相自动识别与应用[J]. 测井技术,2006,30(3):233-236.

[3] 成　敏,朱海华,沈海燕. 射孔资料自动化处理[J]. 测井技术,2003,27(1):59-61.

[4] 吕海霞. 基于 DTW 的相似度查询在完井深度计算中的应用[D]. 大庆:东北石油大学,2011.

[5] 王　萍,唐　澈,马　楠,等. 一种基于虚拟井和多层对比的地层对比方法[J]. 天津大学学报,2009,42(8):744-751.

[6] 李先鹏. 一种基于层序分析的相对深度校正方法[J]. 内蒙古石油化工,2009(14):28-30.

[7] 张　军,李洪奇. 常规测井资料质量自动验收方法研究与软件应用[J]. 天然气工业,2010,30(3):44-47.

[8] 雍世和,张超谟. 测井数据处理与综合解释[M]. 东营:石油大学出版社,1996.

[9] 谢元德. 相对深度法进行校深在现场的应用[J]. 中国石油和化工标准与质量,2012(7):163-163.

[10] 郑恩辉,李　平,宋执环. 代价敏感支持向量机[J]. 控制与决策,2006,21(4):473-476.

[11] Keogh E J, Pazzani M J. An enhanced representation of time series which allows fast and accurate classification, clustering and relevance feedback [C]//Proceedings of international conference on knowledge discovery & data mining. [s. l.]: [s. n.], 1998:27-31.

[12] Domings P. MetaCost: a general method for making classifiers cost-sensitive[C]//Proceedings of the 5th ACM SIGKDD international conference on knowledge discovery and data mining. San Diego, CA: ACM, 1999:155-164.

[13] Grove B, Heiland J, Walton I, et al. New effective stress law for predicting perforation depth at downhole conditions[C]//Proc of SPE international symposium and exhibition on formation damage control. [s. l.]: [s. n.], 2008:13-15.

[14] Basiev T T, Karasik A Y, Osiko V V. Technologies of perforation of closely spaced micron holes with the help of neodymium[J]. Quantum Electronics, 2009, 39(4):385-387.

(上接第 110 页)

[6] Song Lipeng, Jin Zhen, Sun Guiquan. Influence of removable devices on computer worms: dynamic analysis and control strategies[J]. Computers and Mathematics with Applications, 2011, 61(7):1823-1829.

[7] Feily M, Shahrestani A, Ramadass S. A survey of botnet and botnet detection [C]//Proceedings of the 3rd international conference on digital object identifier. Athens/Glyfada, Greece: IEEE, 2009:268-273.

[8] Hua Jingyu, Sakurai K. A SMS-based mobile botnet using flooding algorithm[C]//Proc of the 5th workshop in information security and privacy. Berlin: Springer, 2011:264-279.

[9] Singh K, Sangal S, Jain N, et al. Evaluating bluetooth as a medium for botnet command and control[C]//Proc of the 7th international conf on detection of intrusions and malware, and vulnerability assessment. Berlin: Springer, 2010:61-80.

[10] Knysz M, Hu Xin, Zeng Yuanyuan, et al. Open WiFi networks: lethal weapons for botnets? [C]//Proc of the 31st annual IEEE international conference on computer communications. [s. l.]: IEEE, 2012:2631-2635.

[11] Binsalleeh H, Ormerod T, Boukhtouta A, et al. On the analysis of the Zeus botnet crimeware toolkit[C]//Proc of 2010 8th annual international conference on privacy security and trust. Ottawa: [s. n.], 2010:31-38.

[12] 李　跃. 面向移动网络的僵尸网络关键技术研究[D]. 成都:西南交通大学,2013.

[13] 银河网安官网. 通过移动僵尸网络传播惊现 Android 木马病毒[EB/OL]. 2013-09-11. http://netsecurity.51cto.com/art/201309/410283.htm.

[14] 诸葛建伟,韩心慧,周勇林,等. 僵尸网络研究[J]. 软件学报,2008,19(3):702-715.

[15] Gsma launches sms spam reporting service[EB/OL]. 2010-03-25. http://www.pcworld.com/businesscenter/article/192469/gsma Jaunchesj3ms_spam_reporting_service.html.

[16] Zeng Y. On detection of current and next-generation botnets [D]. Michigan: University of Michigan, 2012.

一种基于 SMS 的移动僵尸网络的设计及分析

作者： 徐建， XU Jian
作者单位： 南京邮电大学 计算机学院,江苏 南京,210023
刊名： 计算机技术与发展 ISTIC
英文刊名：
年，卷(期)： 2016(1)