



BlackEnergy DDoS Bot

Jose Nazario, Ph.D.
Tony Scheid

HTTP Bots

- **No persistent connection**
 - Unlike IRC bots
- **Work with proxies**
 - Uses Win32 APIs to make HTTP requests
- **Next generation of botnets?**

Known HTTP Botnets

- **Machbot - DDoS bot**
 - Rare, tracking about a dozen active nets
 - First noticed in AusCERT DDoS, early 07
- **Barracuda - DDoS bot**
 - Handful of attack commands in October, 2007
 - Just started tracking, about a half dozen
- **BlackEnergy - DDoS bot**
 - Somewhat popular “commercial” DDoS kit
 - Lots of .ru, .ua, and regional DDoS targets
 - Actively tracking about 4 dozen

BlackEnergy

- Russian in origin
- HTTP-based commands
- No exploits

Major Features

- **Encrypted binary**
- **Not open source**
 - Builder EXE modifies unencrypted bot EXE
 - Inserts settings, encrypts
 - Yields encrypted bot
 - AV defeated
- **Can target all IPs for a hostname**

BlackEnergy Kit

- **Reviewed version 1.7**
- **Summer, 2007**
- **Price: about US\$40**

Kit Contents

- **PHP web framework**
 - Authentication, control
 - Communication with bot (stat.php)
 - MySQL-backed config, stats
- **Bot EXE builder, binary**
- **Rootkit - hide bots files, processes**
 - Detectable rootkit


EXE Builder Interface

--[BlackEnergy DDoS Bot]--

Server:
Request rate: (in minutes)

Outfile:

BlackEnergy DDoS Bot; ver 1.7 (with HTT

By: 
allmyhate.host.sk

ICMP Freq:
ICMP Size:
SYN Freq:
HTTP Freq:
HTTP Threads:
TCP/UDP Freq:
UDP Size:
TCP Size:
Spoof IP's: (1 - ON; 0 - OFF)

Build ID:

Default command (if can't connect to server):

Execute after minutes (0 - execute immediatly)

Bot Purpose

- **DDoS**
 - Has support for new binaries
 - New versions have SOCKS features
- **No exploits built in**

BlackEnergy Weaknesses

- **No authorization**
 - Anyone can poll URL
- **No checks enforced on bot or build IDs**
- **Weak “encoding” of commands**
 - Later versions reportedly use some encryption
- **These are easy to work around**

Command Vocabulary

- **DDoS commands**
- **Arguments to “flood” command**
 - ICMP - ping flood
 - SYN - TCP SYN flood, arbitrary ports
 - UDP - UDP flood, arbitrary ports
 - DNS - DNS request flood
 - Data - binary data flood
 - HTTP - rapid GETrequest flood

Other Commands

- **Download function, “get” and URL**
- **Idle**
 - Commands: “stop”, “wait”
- **Go away**
 - “die” command

Communications

- **Bots poll server**
 - Poll interval specified in command
 - HTTP POST message
- **Server replies with base64 encoded message**
- **Message specifies parameters, command, poll interval**

HTTP POST From Bot

```
POST /dot/stat.php HTTP/1.1
```

```
Content-Type: application/x-www-form-urlencoded
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;  
.NET CLR 1.1.4322)
```

```
Host: psamtek.cn
```

```
Content-Length: 31
```

```
Cache-Control: no-cache
```

```
id=xCR2_243AEDBA&build_id=D5729
```

ID is from SMB hostname, C: drive volume ID
Build ID is from botmaster



HTTP Reply From Server

```
HTTP/1.1 200 OK
```

```
Date: Tue, 25 Sep 2007 08:30:13 GMT
```

```
Server: Apache/2.0.59 (Unix) FrontPage/5.0.2.2635 PHP/5.2.3  
mod_ssl/2.0.59 OpenSSL/0.9.7e-pl
```

```
X-Powered-By: PHP/5.2.3
```

```
Content-Length: 80
```

```
Connection: close
```

```
Content-Type: text/html
```

```
MTA7MjAwMDcxMDAwOzA7MzA7MTAwOzM7MjA7MTAwMDcxMDAwI3dhaXQjMTAjeENSml8yN  
DNBRURCQQ==
```

Base64 encode message



Message Decoding

10;2000;10;0;0;30;100;3;20;1000;2000#wait#10#xCR2_243AEDBA

- **Four parts, separated by #**
 - Timing, thread counts
 - Command
 - Return interval (in minutes)
 - Bot ID

Command Flexibility

```
2;2;5;0;2;5;2000;2;20;1026;1#flood syn hywd.info 80#60#xHOST
10;3000;10;1;0;30;10;25;15;2000;3000#flood http
partyofregions.org.ua#5#xHOST
1;999999;888888;0;0;30;1;999999979999999999;1;99999;9999#flood udp;
dns; icmp; http; syn; 77.91.226.6#15#xHOST
10;2000;10;1;0;30;50;50;20;1000;2000#flood syn www.ceag.ru,ceag.ru
80,81,82,83,443,25,22,21,110#10#xHOST
```

- **Commands can be mixed**
- **Some masters choose outrageous values (ie number of threads)**

:: Botnet control

total bot's: 122
bot's per hour: 173
bot's per day: 433
bot's for all time: 1335

statistic by builds
24DB7: 1335

Control bots

Flooders options

ICMP flooder
freq:
packetsize:

SYN flooder
freq:

HTTP-GET flooder
freq:
threads:

UDP and TCP/UDP data flooders
UDP/TCP freq:
UDP size:
TCP size:

Advanced SYN and ICMP options
spoofer sender IP:
attack mode:
max sessions: (for 'drop by timeout')

Command
 [help]
refresh rate: (in minutes)

- Operator has a simple interface
- Help even available! (In Russian)
- Basic stats

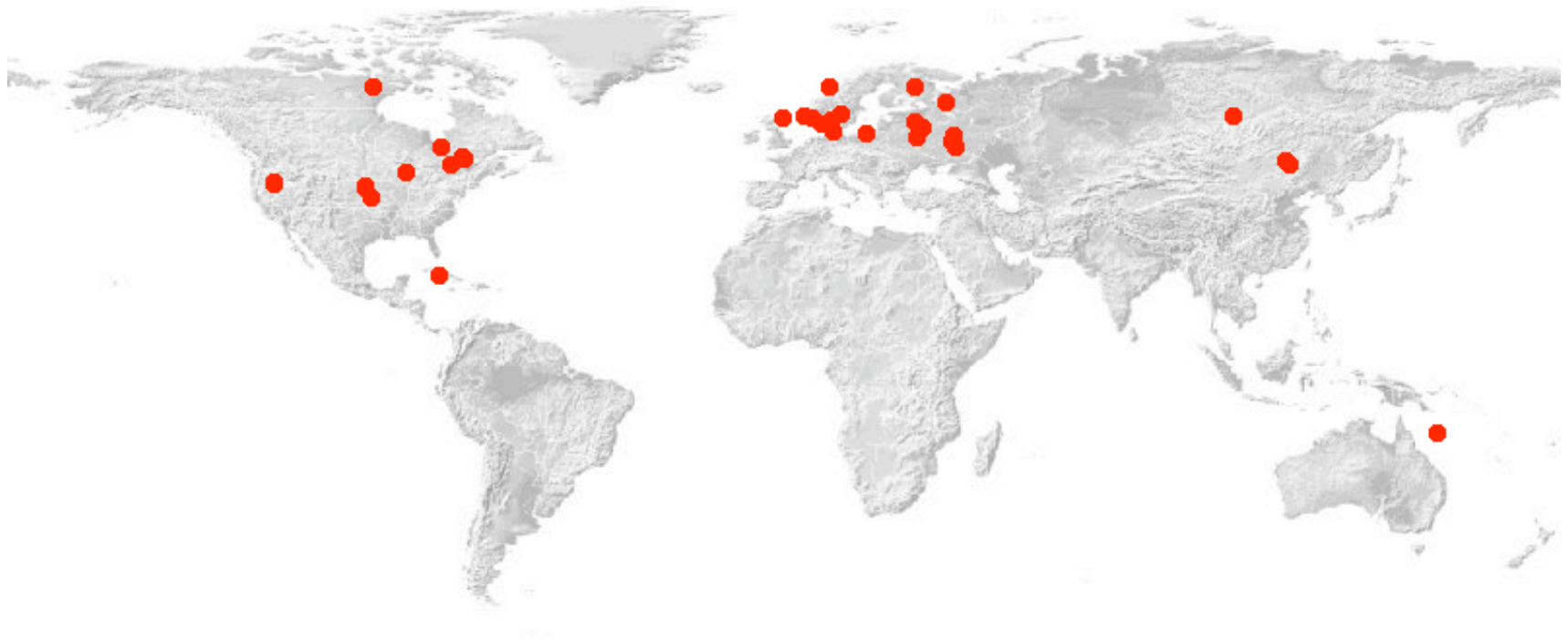
BlackEnergy C&C Locations



33 tracked servers, 11 October 2007

ARBOR[®]
NETWORKS

BlackEnergy DDoS Targets



82 distinct targets, 26 Sep-11 Oct 2007



Blocking BlackEnergy

- We're working with CERTs and ISPs to get known C&Cs killed
- Operators (ISP, enterprise) can:
 - Block by hostname
 - Block by IP and port
- Snort sigs are now available

Our Current Status

- **Have trackers in place for known BlackEnergy C&C commands**
- **Most targets are .ru, .ua sites, underground**
- **Some high profile targets have been hit**