

# ECNet State of The Network Report

Travis L. McArthur

January 16, 2006

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Year in A Nutshell</b>	<b>2</b>
2.1	Bot Floods . . . . .	2
2.1.1	The First Flood . . . . .	2
2.1.2	The Second Flood . . . . .	2
2.1.3	The Minor Floods . . . . .	3
2.2	Software Modifications . . . . .	3
2.2.1	IRCd Modules . . . . .	3
2.2.2	Services Modifications . . . . .	4
2.2.3	BattleServ . . . . .	4
2.3	Operator Abuse . . . . .	4
2.4	Users . . . . .	4
<b>3</b>	<b>The Next Year</b>	<b>4</b>
3.1	Staff . . . . .	5
3.1.1	Training . . . . .	5
3.1.2	Operator Abuse . . . . .	5
3.2	Users . . . . .	5
3.2.1	Advertising . . . . .	6
3.2.2	User Involvement . . . . .	6
3.2.3	Fighting User Disillusionment . . . . .	6
3.3	Technical Advancement . . . . .	6
3.3.1	Coding Committee . . . . .	6
3.3.2	IRCd and Services Modifications . . . . .	7
<b>4</b>	<b>Conclusion</b>	<b>7</b>
<b>5</b>	<b>Acknowledgements</b>	<b>7</b>

## 1 Introduction

In this yearly report I will outline the status of the network as a whole, as well as explain where I see our future and what our plans are in the immediate future and this year as a whole.

This is both a statement of intention, a visionary plan, and a look at the most recent developments in our history. This report is not a guidebook by which I believe we can instantly know how to achieve our goals, but rather an abstract plan which I feel we should seek to fulfill.

## 2 Year in A Nutshell

Our recent anniversary marks out one year anniversary. I will begin this report on our status by stating some of the most prominent developments which have occurred in the past year, as well as our reactions to them and their permanent effects on ECNet as a whole.

### 2.1 Bot Floods

When we look over the past year we cannot avoid looking at the many attacks against our network integrity. The most common form these have taken is that of bot floods. Each flood had specific challenges and unique techniques, and each spawned further preparation. At the end of the series of bot floods, we had achieved numerous anti-bot systems and procedures through which we were able to stifle off many a minor bot flood.

#### 2.1.1 The First Flood

The first major bot flood occurred in October of 2005. This bot flood was coupled with a DDoS. Our servers maxed out at around 75 megabits per second transfer during the worst part of this flood. It effected every user and operator.

When this occurred, only two of our staff were online at the time, and they fought with great speed and did quite well with the tools that were at their disposal. This is also the famed flood wherein the entire operational staff was accidentally banned<sup>1</sup>, but this was quickly fixed without much of an issue.

After this bot flood, we rethought lots of our procedures and security systems. It spawned the movement which eventually led to the removal of the hubs from the DNS to make it harder to attack through DDoS. It also fostered awareness among the staff about bot floods and how to fight them.

#### 2.1.2 The Second Flood

The second major bot flood occurred in November and early December. This flood was triggered by an operator on our network causing trouble for an op-

---

<sup>1</sup>This too, I might add, provided a lesson: be careful with G:line scripts

erator while on another network as a user. This operator asked an individual<sup>2</sup> to attack ECNet with spam messages trying to force us to revoke his o:line and G:line him from the network. We refused to give in, and so the flood continued.

After the initial reaction of mild panic, our staff began standard procedures and banned users entering the public channels that were attacked. We contained the bots to #ECNet and began mass bans. This functioned and did the job, but was not automated.

After only twelve hours the ECNet staff had figured out the most optimal way to ban these bots. Spam filters were put into place matching the text the bots were spamming, and the channel modes of #ECNet were configured as to prevent anyone from joining, but instead putting them in #dump. This channel had a bot that was quickly whipped up which would allow legitimate users to force a join to #ECNet. This made the floods effects minor.

This flood was in reality not a threat and didn't effect most of the network. Hitting only #ECNet allowed centralization of bot fighting efforts and the messages that were used allowed a very simple means to disable them. This flood finally stopped once we spoke to the flooder and he discontinued it on a whim.

### 2.1.3 The Minor Floods

Along with the two major bot floods, ECNet has endured numerous much smaller floods. These floods have come from various sources, but all of them have been repelled by the staff as well as the automated protection systems quickly enough to not become a major concern to us or our users.

## 2.2 Software Modifications

Over the past year we have modified our IRCd as well as services from their stock configuration. We have also developed several of our own home-grown systems to aid in a number of instances. Here I will detail some of the more critical modifications, their causes, and what they have done to help the network.

### 2.2.1 IRCd Modules

We presently run several modules in the IRCds. Individual server admins may elect to install additional modifications providing they get permission first, but the following modifications are required.

- Privdeaf - This module adds the +D umode to allow users and operators to disable private messages
- CGIIRC - This modules aids with our users CGI-IRC installations and the translation to IP addresses

---

<sup>2</sup>For those familiar with the myriad of botnet owners, this specific individual is called '2dcube

### **2.2.2 Services Modifications**

Services have been modified to better reflect our needs. Several features we don't need have been removed, the help texts have been overhauled, and generally it is much more efficient. A few new minor features have been implemented, but nothing significant enough to mention here.

### **2.2.3 BattleServ**

BattleServ was a system programmed by ECNet staff members to help fight bot floods. It has two primary functions to fight the bot menace.

First of all, it runs a channel that is used to catch bots who join the most populated channels. Anyone who joins this channel has their connection frozen, and BattleServ will announce this to the operators so they know. This has led to some false positives, but overall has been very effective.

Secondly, BattleServ is equipped with a pattern matching system which scans all users when they login and checks for certain known fingerprints of bots. If these are found, it freezes their connection and announces it to the operators so that they may deal with it further.

BattleServ has been indispensable in fighting minor and major flood alike. There are plan to improve and expand BattleServ to further protect the network.

## **2.3 Operator Abuse**

Over the past year our team has grown quite large. We have faced only one major difficulty with the growth in team members: abuse. While cases of abuse have been isolated, they have still existed. Each of the three documented cases of operational power abuse have been handled by the abuse committee, and they have done an excellent job of it.

## **2.4 Users**

Since our inception a year before, we have linked multiple servers and had many users move their channels to our server. So far, we have yet to have a channel leave us once they arrive. Our service and our identity are a guiding principle to us, and has been since we began and has helped to bring users. We currently have online between 150 and 180 users at any given time.

## **3 The Next Year**

Now that our first year is over, we have seen all that can be accomplished with determination, patience, and many bottles of caffeine laced substances. As we enter our second year, we must strive to expand and grow, to not allow our success to lead down the road to stagnation which at its end has a sad fate. We must not forget who we are and were, and where we cam for, and yet we must strive to be more than we are. Here I will try to explain my vision as the lead

network administrator for this year, and what I feel our immediate goals should be.

### **3.1 Staff**

Our staff has grown this year from three people trying to run a network to a group of operators and admins in excess of 20 people. This growth has had many positive effects and means that we have much more manpower and capability. This also means, however, that we should look towards our staff, as great as they are, and find ways to improve ourselves.

#### **3.1.1 Training**

Most staff members are highly trained in what they do, but not all are equal. What I would like to propose is that sometime within this year we start an informal group of individuals who are charged with training of the staff. This training would cover the more advanced IRC operational commands as well as IRCd internals. This training would help operators who wish to learn more<sup>3</sup> than they already do and have the time to do it. These individuals would have to be volunteers because such a process would be very time intensive and would have to be scheduled around other commitments. Such a training system would significantly increase our operational staff's capability to respond efficiently and in the best possible way when emergencies occur.

#### **3.1.2 Operator Abuse**

Over the past year we have had only three incidents of operator abuse which have gone far enough to be reported to the abuse committee. All three were handled promptly and appropriately. The way we handle abuse is excellent, and honestly I cannot think of a single way to improve it, we simply must remain diligent and professional in the way we interact with users and each other, so that we do not lose what we have strived so hard to create.

### **3.2 Users**

Our users are the core of what we do, without them all that we do and all that we build has no meaning. As such, we should try to retain that from the past year which has been positive, including our sense of kind professionalism and informal friendliness with our users. While doing this, we should also make broad new measures to attract users and further encourage the ones we have. To do this I would like to propose several new measures.

---

<sup>3</sup>Not to mention names like Stitch.

### **3.2.1 Advertising**

As many of you may know, we already have small advertising campaigns<sup>4</sup>. I would like to suggest that we begin a larger targeted advertising campaign. We will not spam anything, but we will try to spread the word about ECNet. Doing so will bring more users in questioning, and when they find out what we're about they will probably stay.

### **3.2.2 User Involvement**

As time goes on, we should work to involve users who are interested in the internal operations of the network. We must preserve security of the network above all else, but that does not mean that we can't discuss trivial operational details with users. Often this is a good way to locate candidates for staff positions as well as foster a sense of the operational staff being part of the network community.

### **3.2.3 Fighting User Disillusionment**

One of the things we must not let happen is an unhappy user, unless absolutely necessary. When a user gets angry at us as a whole, disillusioned with how we run the network, either the user has been incredibly unreasonable in their expectations, or we have failed to provide what we said we would: a good place to chat.

There are times when we must just tell users to go away and stop being idiots, but many times users are simply frustrated at what has happened. Often they will be mad at us because they think we're responsible for them being banned from a channel, or because they were killed for some abuse. We must try to explain to them calmly and coolly what happened and why, and try to satiate them. This is not an easy thing to do, but it is something that we as operators are obligated to do.

When you get too tired, angry, or just plain sick of it all to do this, it is time to log off or deop for a while, and just let yourself cool down. There is no dishonor from backing away from something you can't deal with except at the cost of blowing your top.

## **3.3 Technical Advancement**

So far we have customized much of our services and IRCds to our liking. I would like to suggest that we push further forward with this initiative of customization. For this purpose, I have several measures I would like to propose.

### **3.3.1 Coding Committee**

Under the powers proscribed to me in the ECNet constitution article two section a, I hereby authorize the creation of a coding committee. The coding commit-

---

<sup>4</sup>One of these thanks to nos-x

tee's charter will be written and activated as of Monday, January 16, 2006. This committee will be charged with coding and maintenance of BattleServ, services, and custom IRCd modules. It will have to have all suggested changes approved by the infrastructure committee prior to the modifications being made. Once modifications are made and tested, such modifications will be made mandatory after a four week period. The members of this team and how new members may be added will be explained when the team charter is released.

### 3.3.2 IRCd and Services Modifications

With the coding committee formed, I would like to recommend we begin additional work on IRCd and services modifications to remove those modes and features we do not need, and add those we do. As such, I would like to ask all users and operators to report to myself or any other ECNet staff members any new ideas for the IRCd or services features.

## 4 Conclusion

With this report, I have explained what I feel is the critical points of our past, as well as what I see for our immediate future. This report is less of a definitive answer to the question "Where are we going?" but more of an answer to the question "where do you think we should be?"

## 5 Acknowledgements

*The author would like to thank the following people on behalf of ECNet:*

Larry Titus  
James Woods  
Jeremy Sayres  
Benjamin Smith  
Claire Naylor  
Eugene Haller  
Juan Pablo Cugnini  
And The ECNet Users