SANS ISC

Bots e Botnets

Pedro Bueno, SANS GCIA

SANS Internet Storm Center

pbueno@isc.sans.org / bueno@ieee.org

GCIA

GIAC CERTIFIED INTRUSION ANALYST

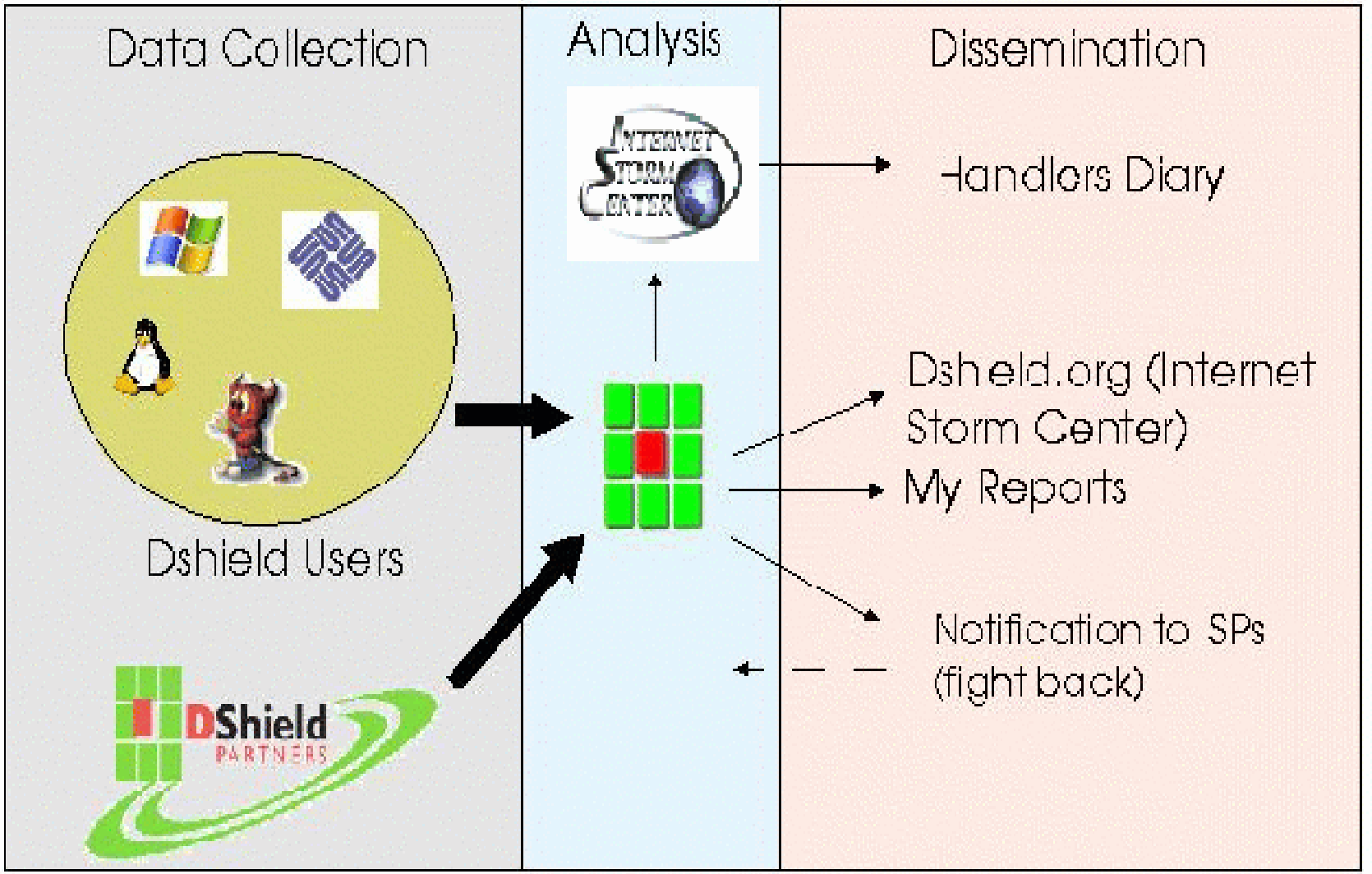
“Malware development is accelerating due to efficient and open collaboration, moving from months and years to weeks and days”

--Johannes Ullrich, CTO do SANS Internet Storm Center (ISC)

Agenda

- Introdução ao ISC
  - Sensores Distribuídos e DShield.org
  - Analise dos Dados e a Lista dos Handlers
- Bots
  - Variantes AGO/PhatBot
  - Caso Veritas
- Botnets
- Conclusões
- E ainda...Apresentando a NSP-SEC-BR!

O Internet Storm Center



Participação

- Enviando Logs de Firewall

  - Suporte à um grande número de firewalls. Para uma lista atualizada e instruções, veja:

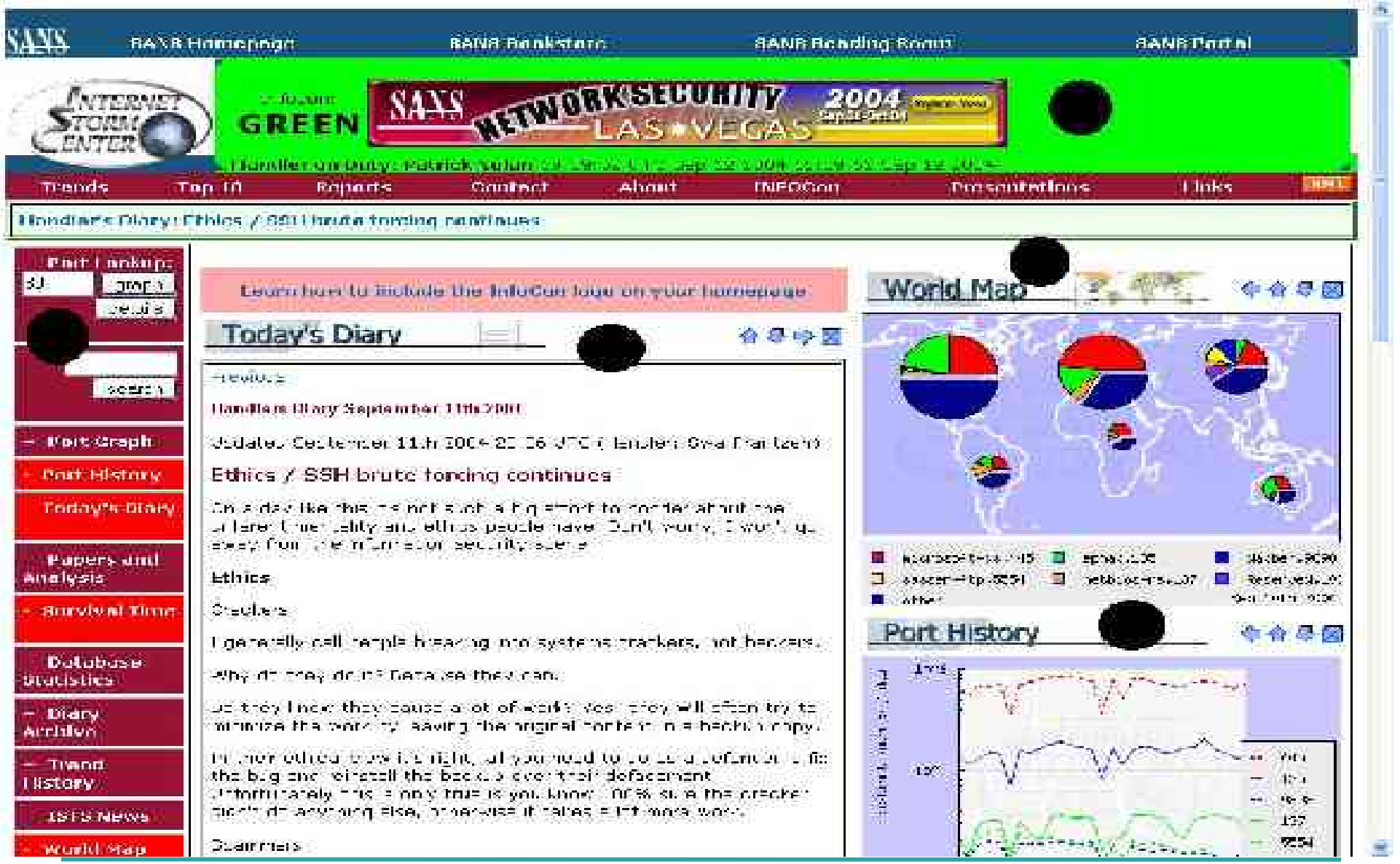
    http://www.dshield.org/howto.php

  - Os envios podem ser feitos de forma anônima. O importante é lembrar que nenhuma rede é pequena para o envio destes Logs!

- Relatando incidentes para o time de Handlers do SANS ISC.

  - Estranhos binários encontrados, sinais de exploits, dicas para prevenir incidentes, ou mesmo para instruções para os usuários.

Entendendo o website do ISC



http://isc.sans.org

Handlers List

- Grupo de 30 profissionais de segurança
  - Geograficamente dispersos (América do Norte e Sul, Europa, Asia)
  - background (ISP, governo, financeiro, educacional)
- A cada dia um handler é designado a ser o 'handler do dia‘
- Para enviar noticias, dúvidas ou questionamentos aos handlers, utilize o formulário de contato(http: // isc.sans.org/contact.php)

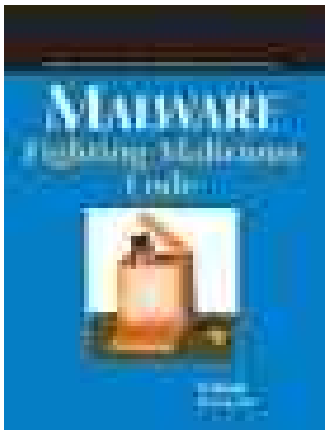
Malwares

- Bots são Malwares...mas afinal...o que é um Malware?

"Malware is a set of instructions that run on your computer and make your system do something that an attacker want it to do."

--Ed Skoudis

ISC Handler e Autor do livro Malware: Fighting Malicious Code



Bots

- Por que vimos uma onda de Bots/Malwares em 2004?
  - Em abril de 2004, mais de 900 variantes do GaoBot

Virus Characteristics:

-- Update August 11, 2004 --

There are now over 4000 variants of this threat, many of which were proactively detected, and this number continues to grow at a rapid rate.

AVLab is constantly enhancing generic detection for this family. To ensure you have appropriate protection please do use the latest DAT's, latest engine and do not disable scanning of packed executable files.

Update April 6, 2004

There are now over 700 variants of this Trojan-infected worm. Multiple new variants are discovered each week. They vary in file size and name.

This detection is for worms that are based on the IRC Sdbot trojan code. The source code for the IRC Sdbot trojan was published on the Internet some time ago, and a number of worms are based on the same code. The following are such worms:

- W32/Sdbot.worm
- W32/Sdbot.worm.gen
- W32/Sdbot.worm.gen.h

- 50 variantes por semana

Large Numbers of Gaobot Worm Variants Proliferating
April 29, 2004

McAfee Thursday issued an alert for W32/Gaobot.worm.al, with the warning that there are more than 900 variants of the Gaobot virus in existence.

The source code for Gaobot was posted to various web sites resulting in many new variants being created each week, the vendor reported.

W32/Gaobot.worm.al stands out from some others as it seems to be the first variant that incorporates code to exploit a MS04-011 vulnerability (LSASS Vulnerability (CAN-2003-0533)). This particular variant is not currently a threat as it is dependant on an IRC server, which is no longer available. However, it is presumed that other variants will likely follow soon, which are functional. Details of those variants will likely vary from this one.

Bots

...em 2005:

De Janeiro a Junho de 2005:

4268 Novas Variantes de Bots!

Fonte: F-Secure

Agobot * Spybot * Aebot * Aimbot * Alcobot * Babot * Badbot * Bbot * Bigbot * Evilbot * Gobot * Msbot * ShellBot * Psybot * Rbot * Sbot * Sdbot * Aebot * GTBot * Nyrobot * Robobot * Rsbot * Vbbot * Padobot * Kazabot * Gunbot * IRCBot ...

Caso Mytob = Mydoom + SdBot

http://isc.sans.org

Caso Veritas

- Vulnerabilidades no Software Veritas
  - 6 Security Advisories lançados em 22 de Junho de 2005

    - 22.06.2005 : Veritas Backup Exec Remote Agent Privilege Escalation Vulnerability
    - 22.06.2005 : Veritas Backup Exec Admin Plus Pack Option Remote Heap Overflow
    - 22.06.2005 : Veritas Backup Exec Web Administration Console (BEWAC) Vulnerability
    - 22.06.2005 : Veritas Backup Exec Server Remote Registry Access Vulnerability
    - 22.06.2005 : Veritas Backup Exec Remote Agent Buffer Overflow Vulnerability
    - 22.06.2005 : Veritas Backup Exec Remote Agent Denial of Service Vulnerabilities

Caso Veritas

- **VX05-006** June 22, 2005
  Remote Heap Overflow when using the VERITAS Backup Exec Admin Plus Pack Option
- 2005-06-24 : **Veritas Backup Exec Agent "CONNECT_CLIENT_AUTH" Request Exploit**
- **[** 06/24/2005 **] New exploit module added: backupexec_agent**

```
'UserOpts' =>
{ 'RHOST' => [1, 'ADDR', 'The target address'],
   'RPORT' => [1, 'PORT', 'The target port', 10000],
},
```

Caso Veritas

Report recebido pelo SANS ISC em 28 de Junho de 2005:

"Hello,

We have identified and isolated a new SDBot variant that appears to be trying to exploit the new Veritas vulnerability.

Systems that are infected start sweeping the network looking for port **10000**. The program is recognised by McAfee 4522 (but not by 4521)

The malware was downloaded from:

http://xxx.xxx.xxx.xxx/upload/xxxx.exe

The owner of the site has been notified via e-mail.

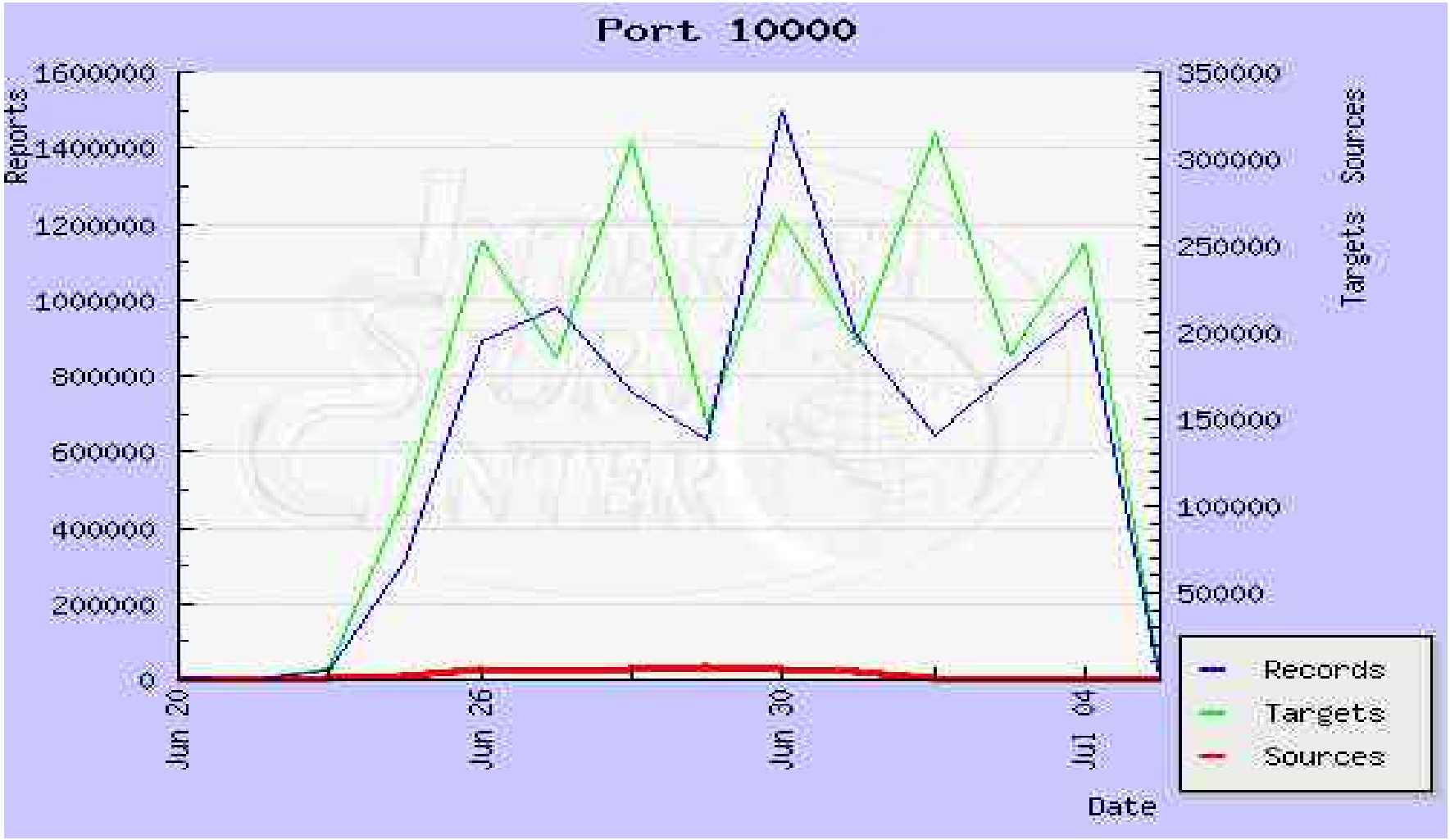
Regards,"

Malwares e o ISC

- Detecção de novas tendencias de Bots
  - O ISC recebe cerca de 40 milhões de Logs por dia e 1 bilhão por mês, o que facilita a detecção de novas tendências.
  - Triggers que avisam quando determinados padrões ultrapassam um limite ou saem de um padrão já observado
  - Gráficos e dados que ilustram as mudanças de comportamentos de tráfego.

Malwares e o ISC

- Exemplo 1: Porta 10000 – Cisco VPN/Veritas



Criação de Malwares

- Bots!
- Software que realiza ações em nome de um humano
- Não muita diferença dos worms
- Permite um controle remoto da maquina através de IRC (Internet Relay Chat)...
- Vários propósitos:
  - DDoS
  - Relay para Spam
  - Proxy Anônimo
  - Controle total da máquina via IRC
- Vários bots sob o dominio de um atacante == BotNet

Criação de Malwares

- 2004: O ano dos Bots!
  - AGO/GAObot, Phatbot, SDbot, RxBot, rBot, SpyBot, Global Threat...
- Busca por:
  - Múltiplas vulnerabilidades,
  - Backdoors deixadas por outros vírus (MyDoom...)
  - Múltiplas portas abertas para realizar o ataque:
    - 2745, 1025, 3127, 6129, 5000, 80...
- Nosso exemplo:
  - AGO/GAObot
  - Phatbot

Agobot == Gaobot == Gobot == Polybot == Phatbot

Criação de Malwares

- Família Ago/Gao/PhatBot
- Características:
  - Base de conhecimento de exploits:
    - Porta 135 – exploits antigos
    - Porta 445 – exploits antigos
    - Porta 80 – exploits antigos IIS
    - Porta 3127 – Backdoor MyDoom
    - Porta 2745 – Backdoor Beagle
    - Porta 6129 – exploit para Dameware
    - ...
    - Incorporação do exploit do LSASS dias antes do Sasser!
  - Controle via IRC de forma anônima
  - Podem fazer “sniffing”...

Port Summary - 4-2004

Top 10
Top 50
Top 75
Top 100

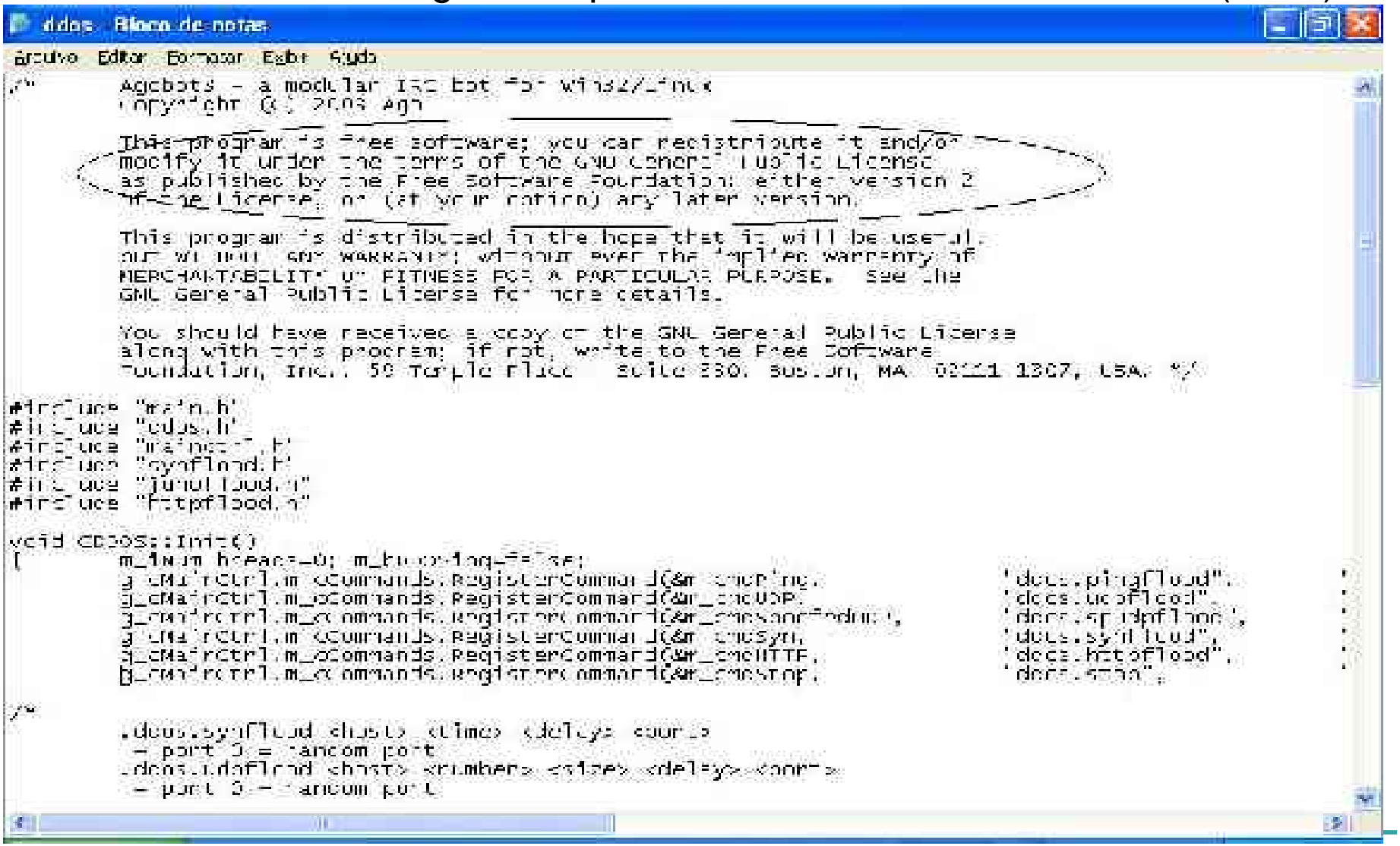
Port	Sources	Targets	Count
135	156051	139819	5133275
445	453076	129243	3778151
80	564585	115219	4276722
3127	55487	111672	1076421
137	39163	110703	1084706
2745	66948	93371	890011
1434	26558	92144	521907
1433	5265	75170	704304
6129	38212	69662	499312
139	39451	68516	603041

Criação de Malwares – Caso Bots

- Por que esses bots representam uma evolução na criação de Malwares?
  - Versões com código fonte parcialmente disseminado e ´livre´
  - Possibilidade de alterar o original, fazendo sua própria variante!

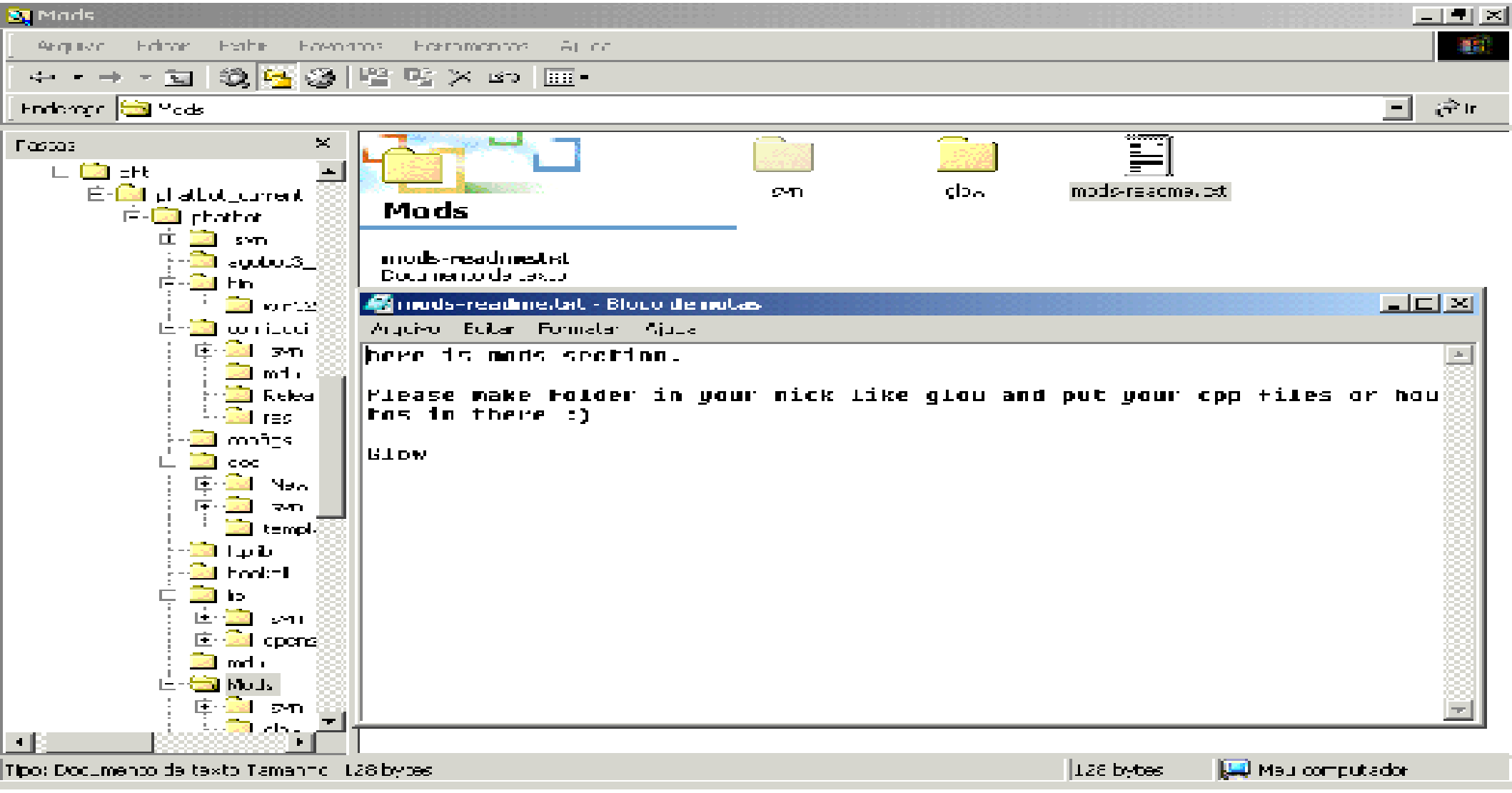
Criação de Malwares

- Versões com código fonte parcialmente disseminado e ´livre´ (GPL!)



Criação de Malwares

- Possibilidade de acrescentar módulos com novas funcionalidades e exploits, chamados de “Mods”

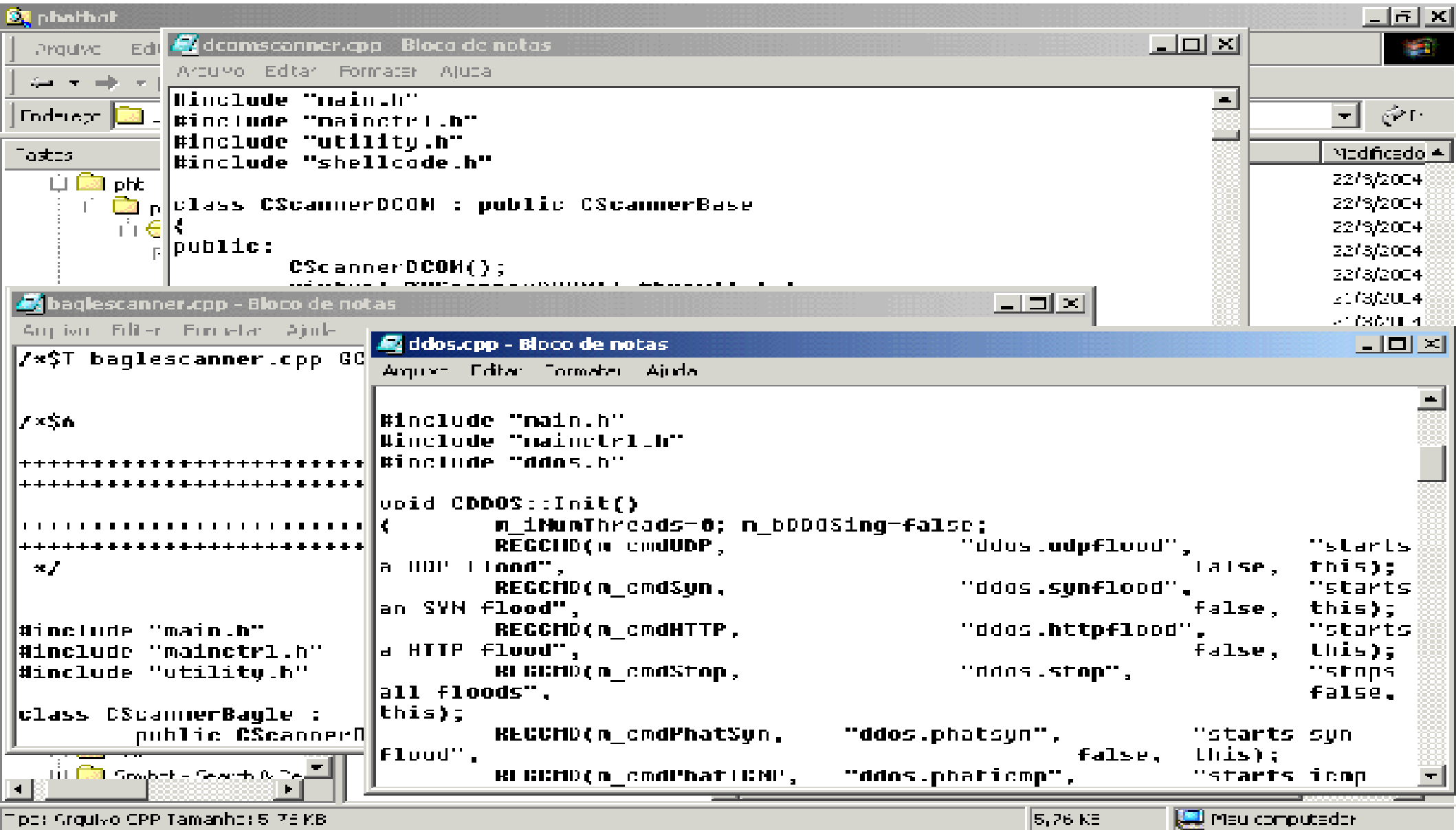


Criação de Malwares

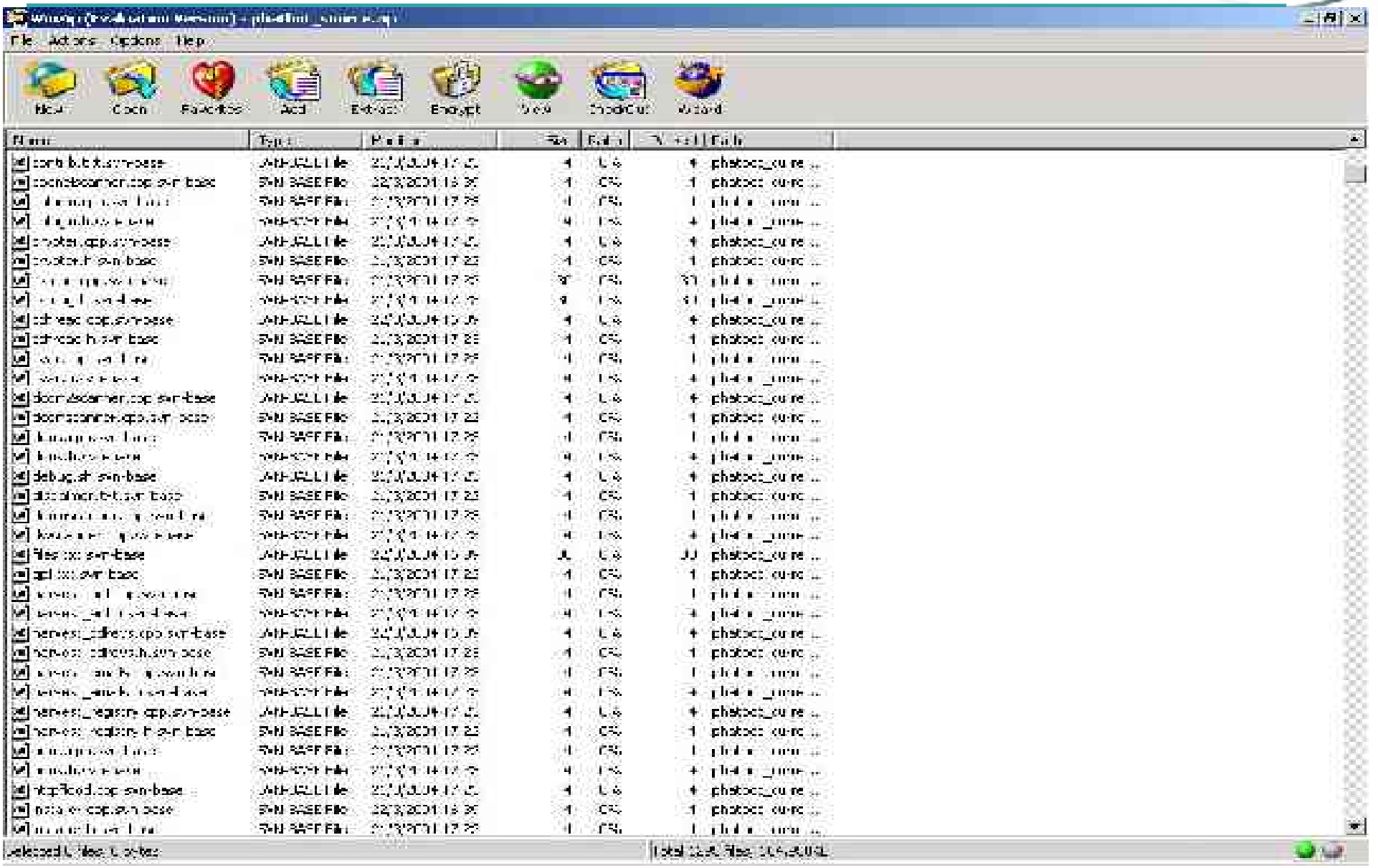
- Referência dos Comandos:

Criação de Malwares

- Modificação fácil do código fonte



Criação de Malwares



http://isc.sans.org

Criação de Malwares

- Muitos arquivos de códigos fontes
- Muitos arquivos de headers
- Muitos arquivos de configuração
- Muitos parâmetros de configuração
- Muitos Mods

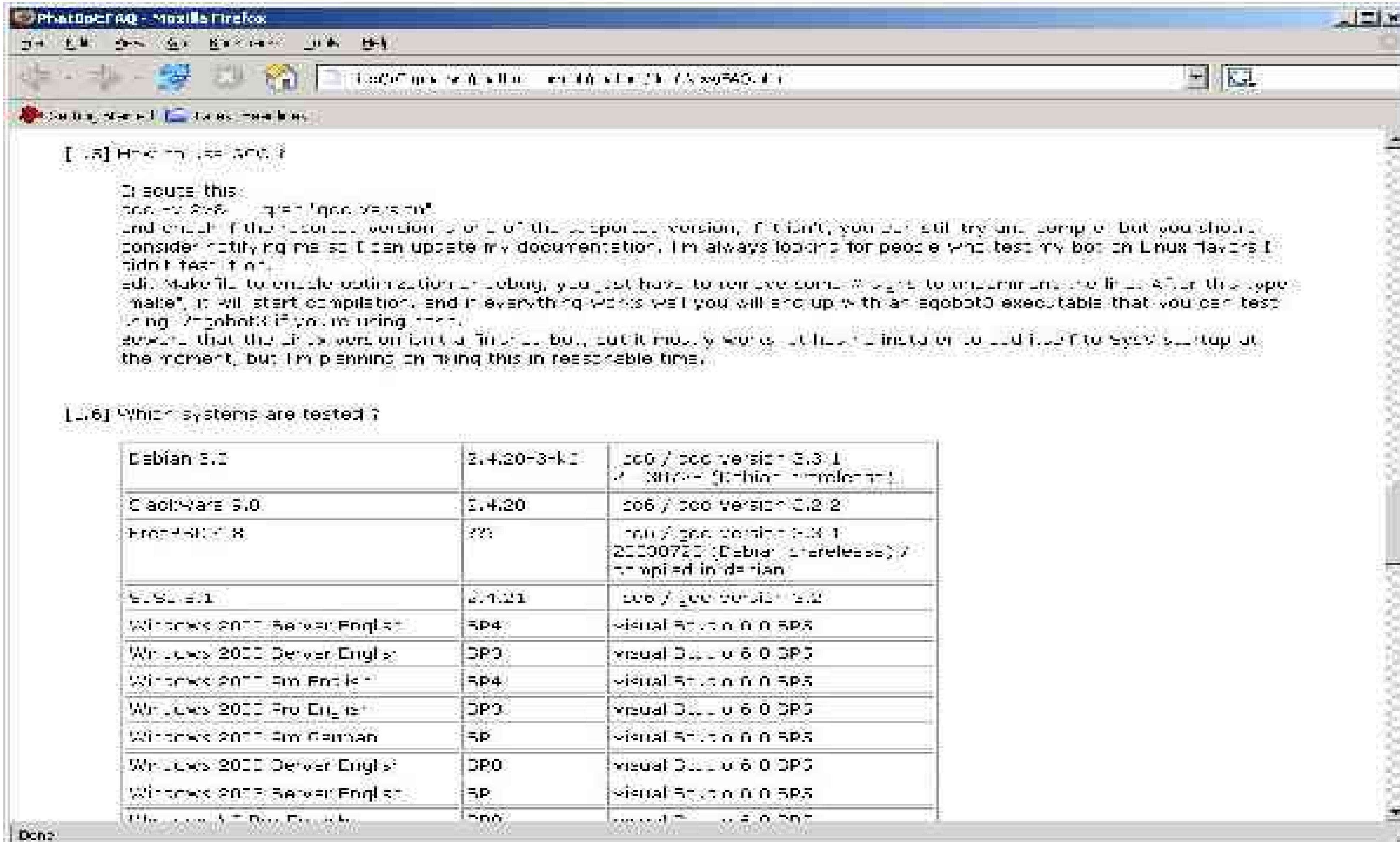
- Enfim...

- Muito complicado criar sua própria versão...

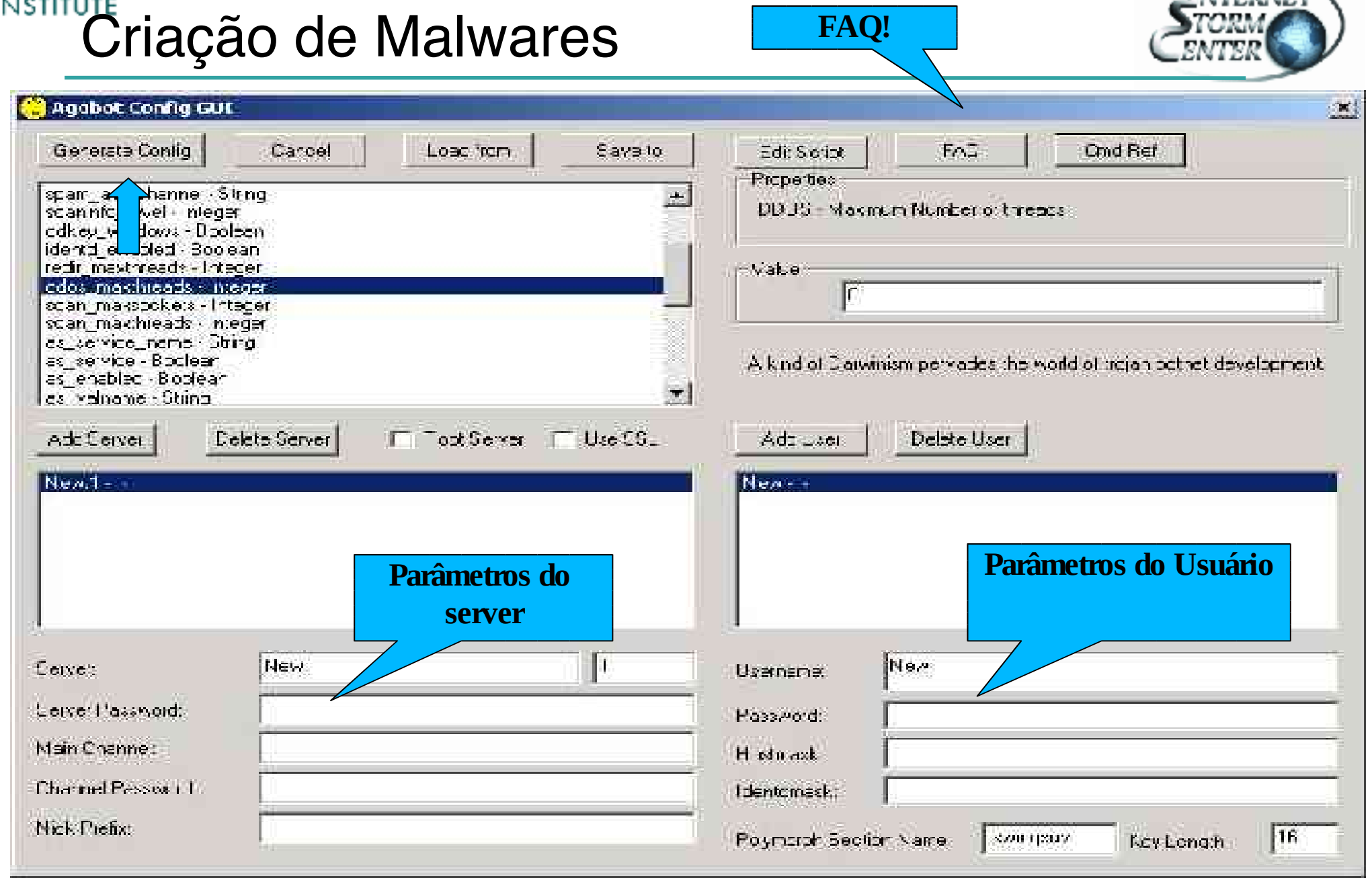
Criação de Malwares

- Mas o boom dos bots é justificado:
  - FAQ
    - Compilação
      - Em Win32
      - Em Linux – instruções do uso do GCC
    - Detalhamento dos módulos
    - Plataformas Testadas

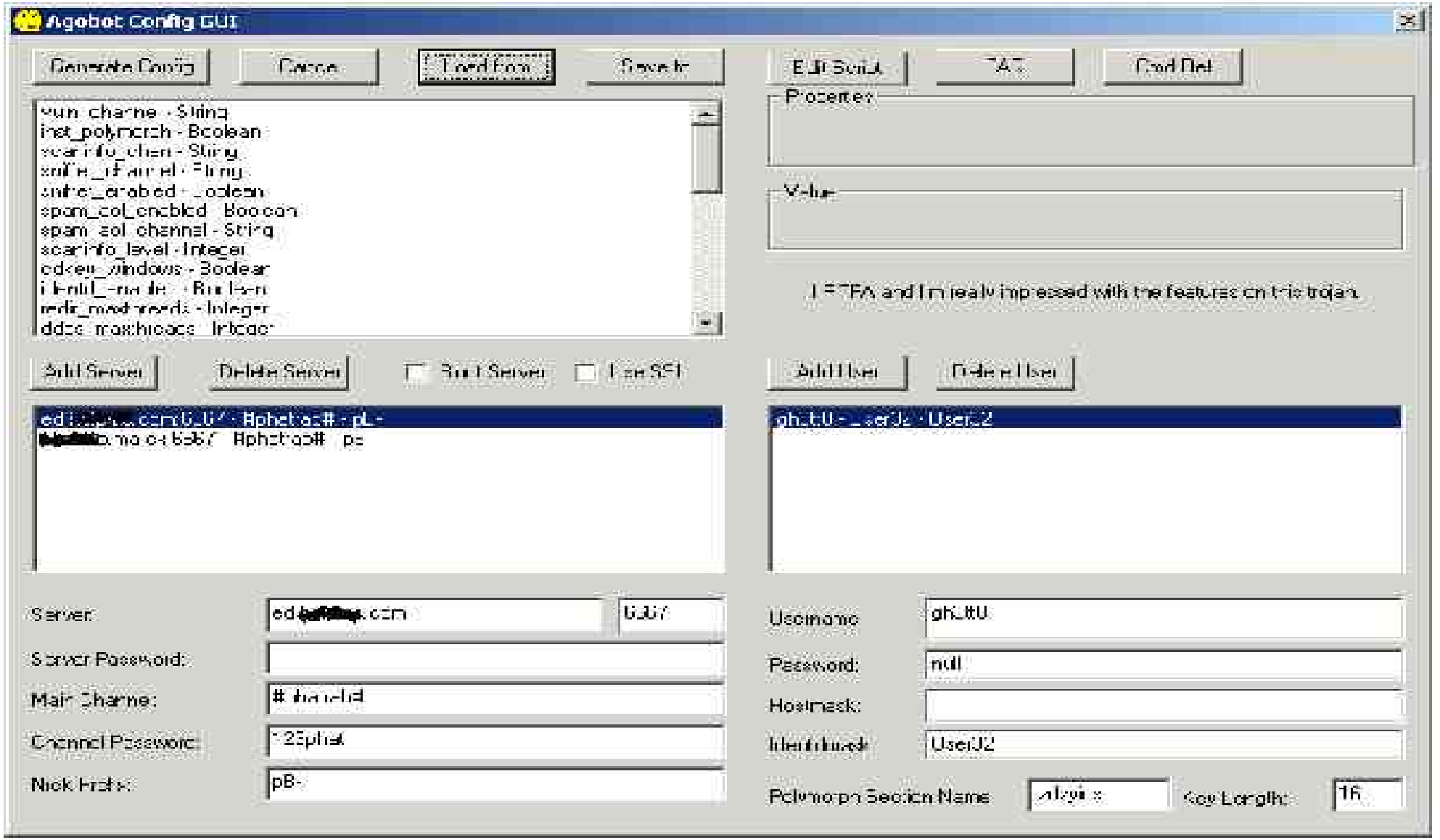
Criação de Malwares



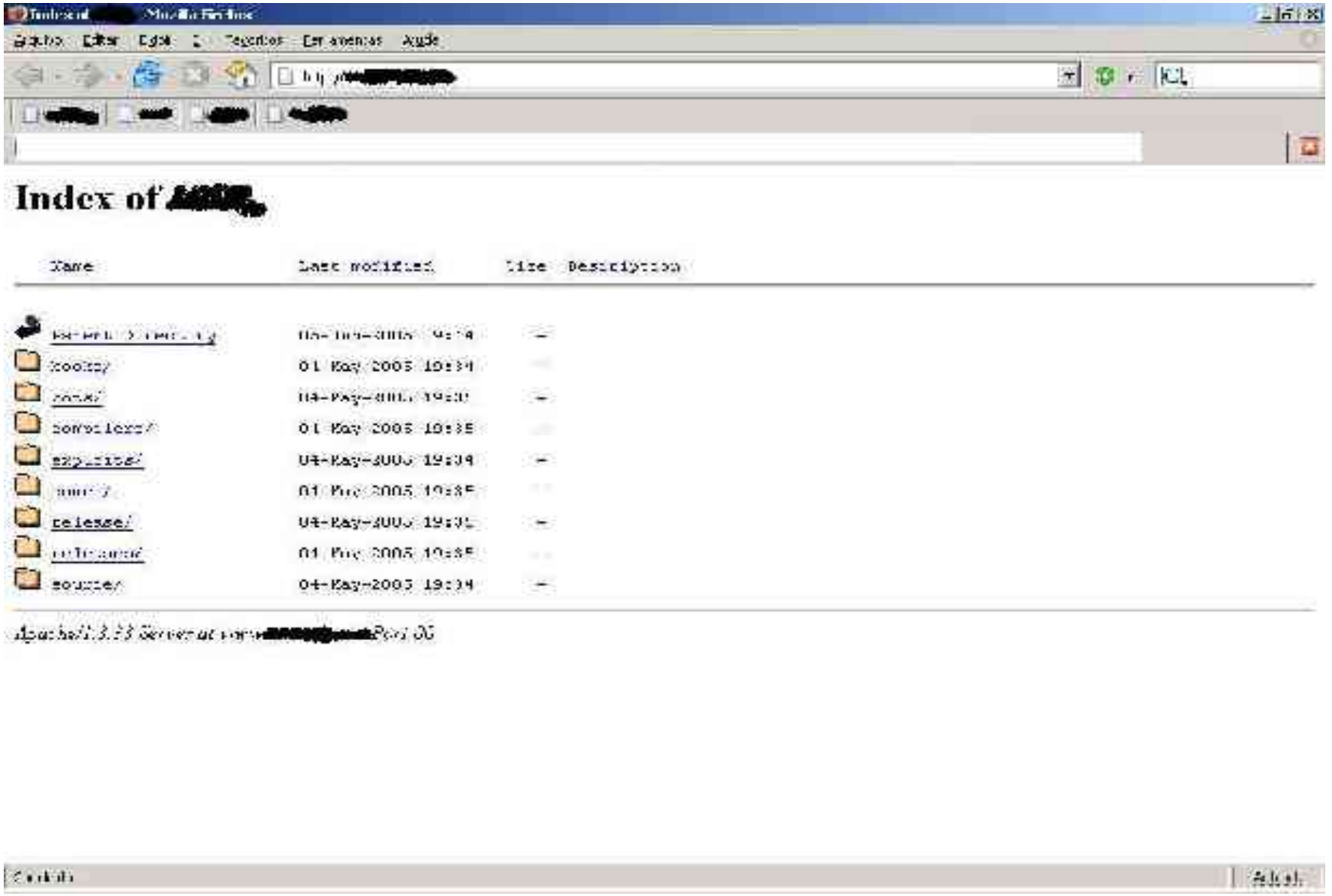
Criação de Malwares



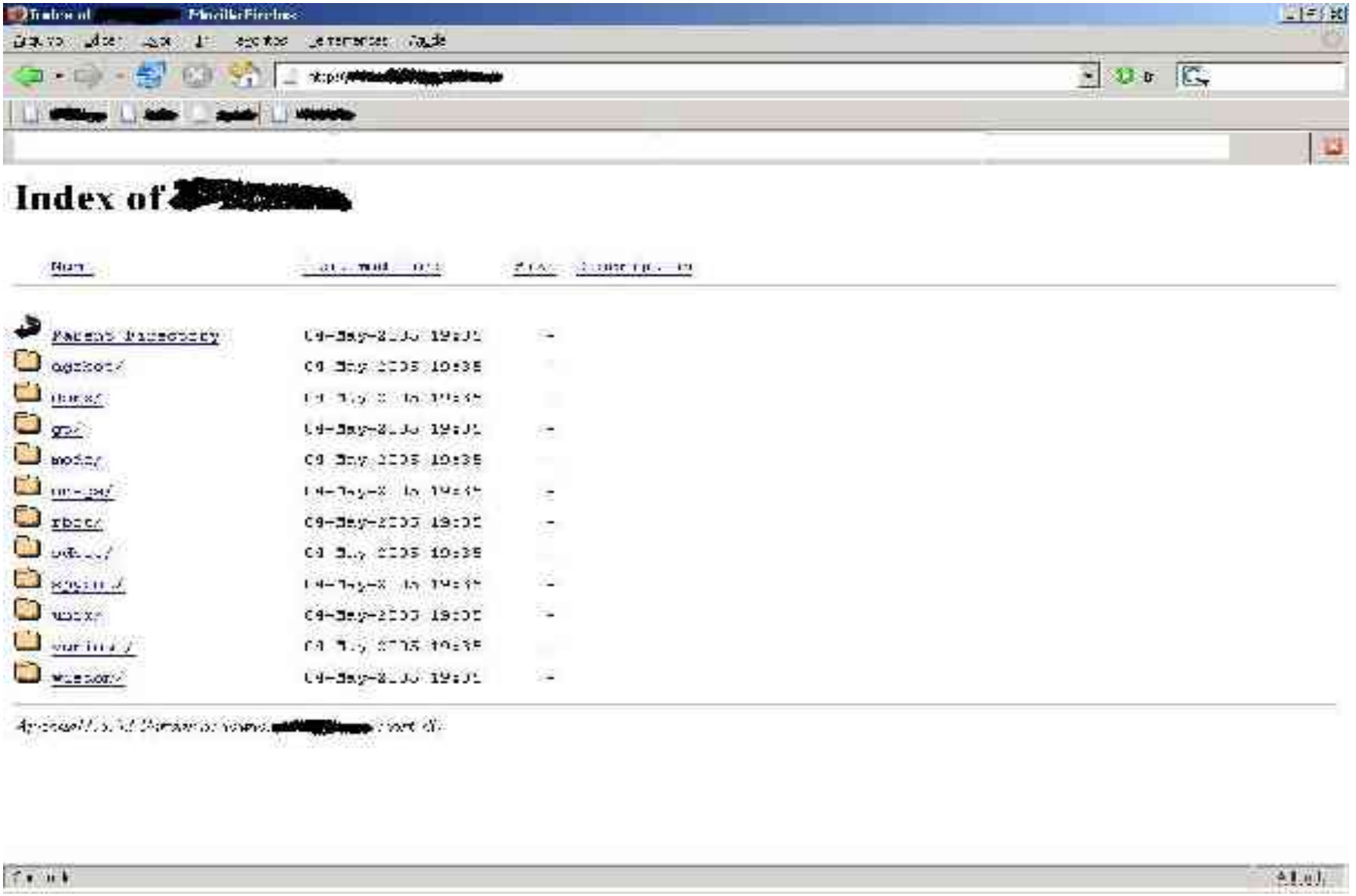
Criação de Malwares



Repositórios de Bots



Repositório de Bots



E não é só isso...

Bots em perl...

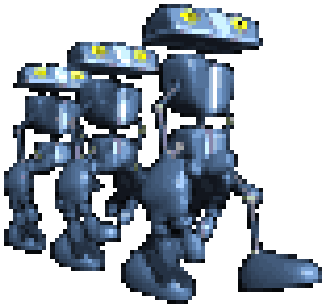
- O Brasil é um dos lideres em bots em perl.
- Report recebido pelo SANS ISC em 17 de Março:

```
“Hi,

Just discovered this attack against one of our IDS customers. The attacking IP.

Xxx.xxx.xxx.xxx.

It's another bot. IRC server at: linuz.xxxxxxxxxxx.net

Channel xxxxxx seems to have been removed, however the file are still available at

xxx.xxxxxxxxxxx.org

Regards, xxxx@xxxxxx

Content :
```

```
“my $processo = '/usr/sbin/httpd';

$0="$processo"."\0"x16;;

my $pid=fork;

exit if $pid;

die "Problema com o fork: $!" unless defined($pid);”
```

Botnets

- Simples:
  - Vários bots sob o domínio de um atacante == BotNet



Botnets permitem ataques de DDoS de vários tipos:

- Ataques ICMP;
- Ataques TCP;
- Ataques UDP;
- Ataques HTTP (Reload, Reload, Revolutions, Reload...);

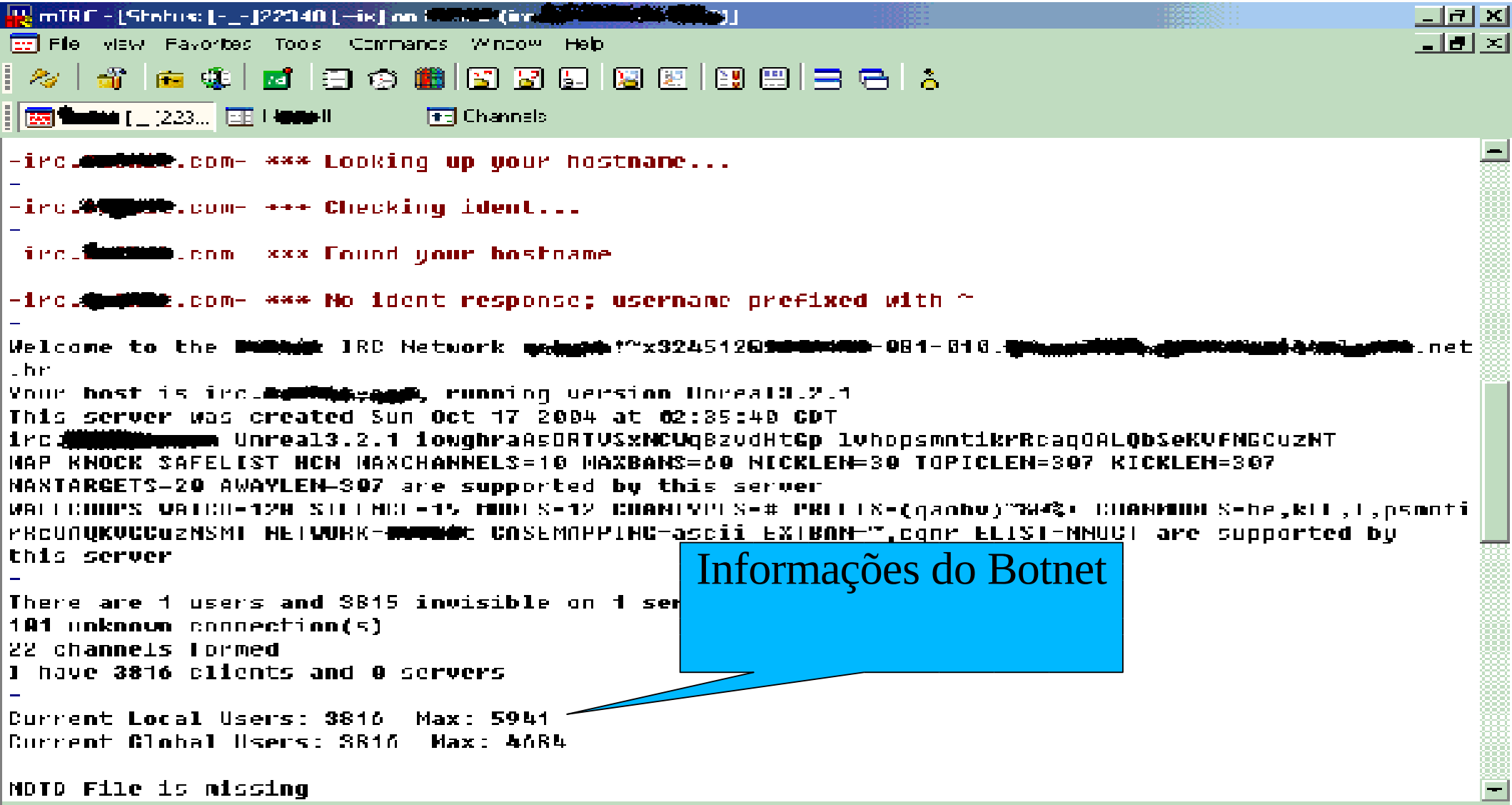
Botnets

- “Controle Remoto” por canais de IRC
  - Internet Relay Chat
  - Servers, Canais, Nicks, Senhas...
- Identidade do Owner permanece “Anônima”
  - psyBNC??
- Portas padrões do IRC: 6665-6669, sendo a mais comum 6667
  - Quem bloqueia a porta 6667 ?
  - ...e as portas 9991, 1122, 9999...???
- Tamanhos variados : 500 bots até 150k bots!

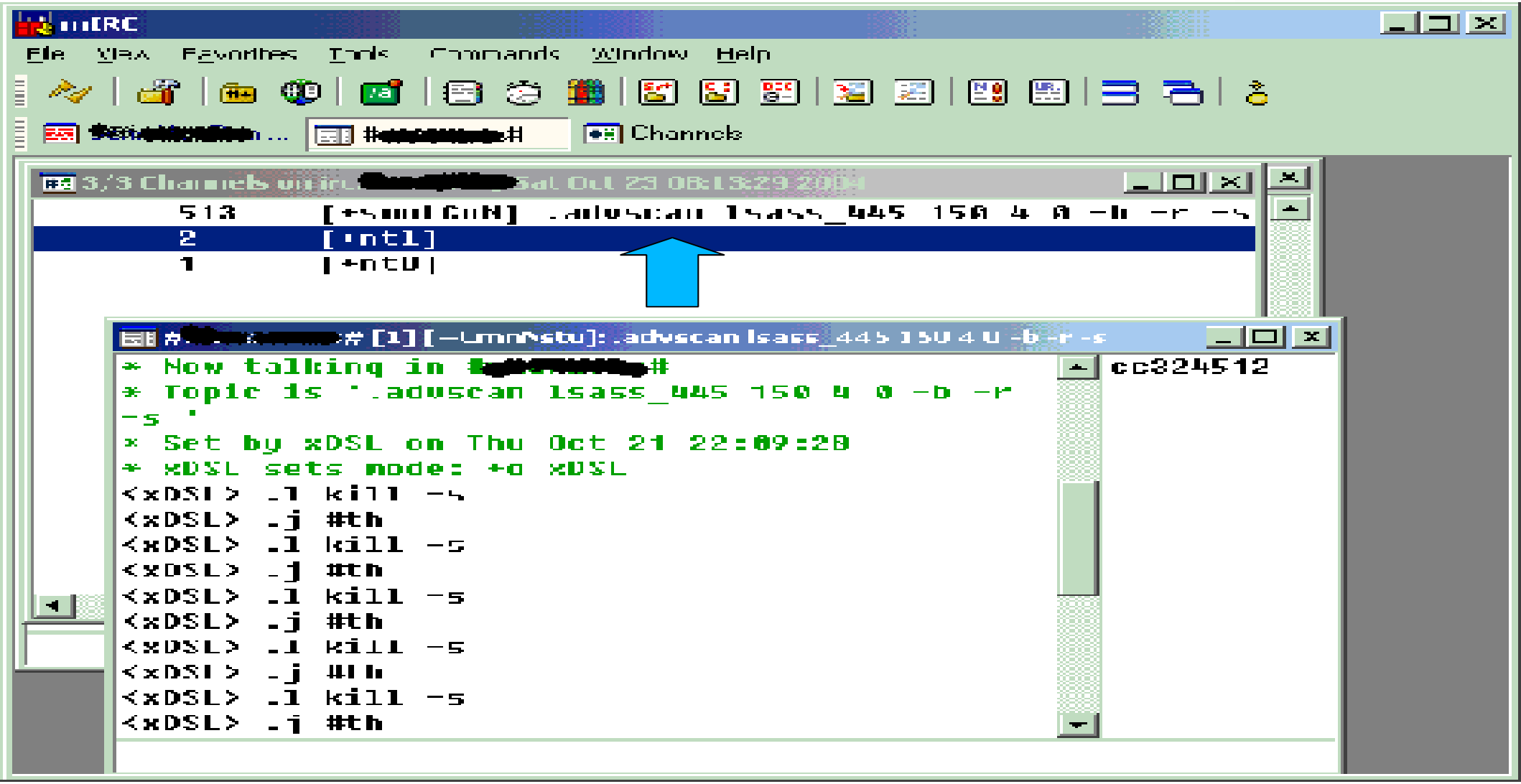
Botnets

- Mas...qual o objetivo?
  - Lucro (algumas botnets são criadas apenas para serem vendidas)
    - Spam, PWS...
  - Pirataria (warez, videos, livros...)
  - Lucro (DDoS for hire!)
    - “Quer pagar quanto!?”™

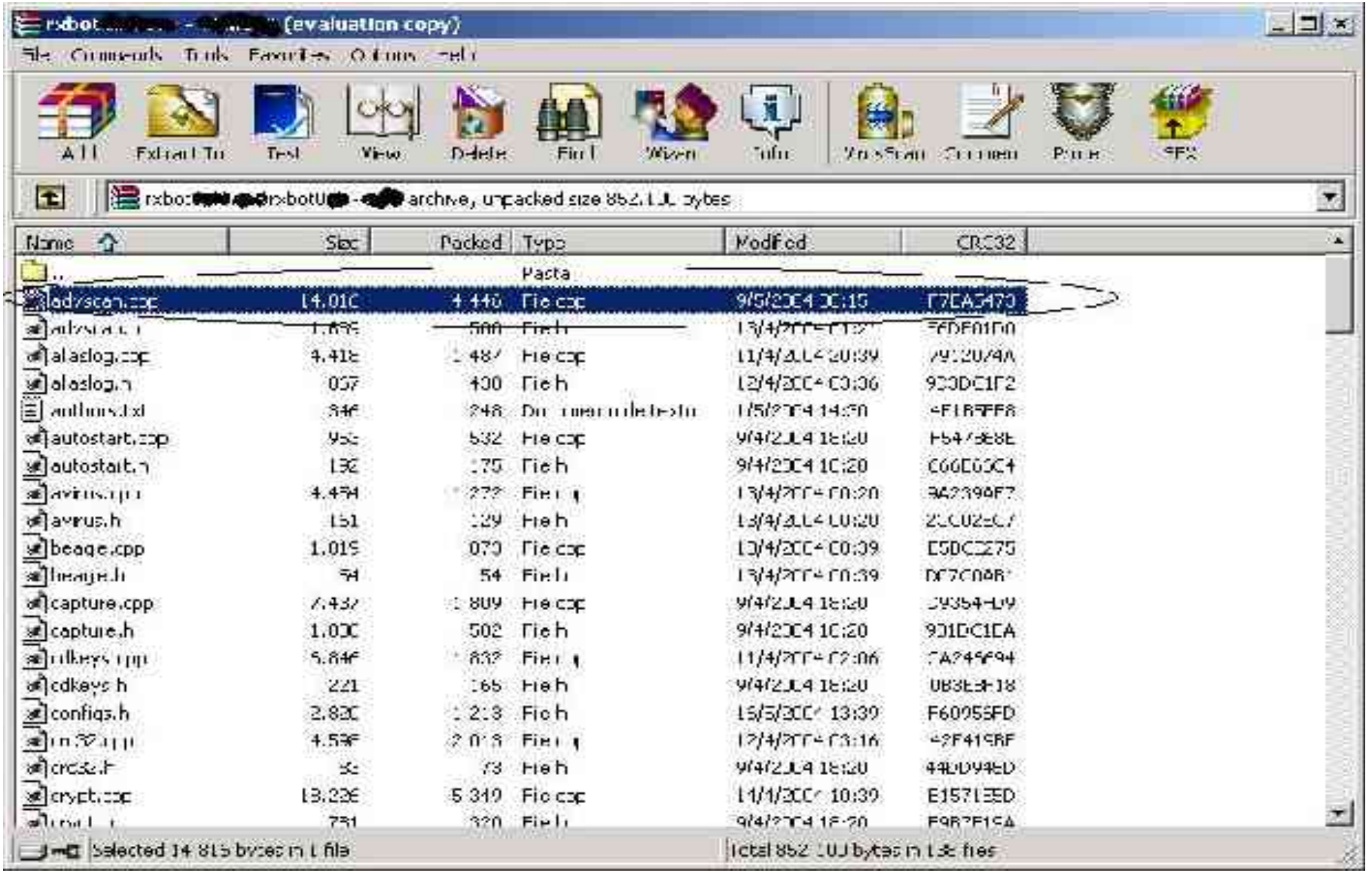
Botnets


File View Favorites Tools Commands Window Help
Channels
-irc.[redacted].com- *** Looking up your hostname...
-irc.[redacted].com- *** Checking Ident...
irc.[redacted].com *** Found your hostname
-irc.[redacted].com- *** No Ident response; username prefixed with ~
Welcome to the [redacted] IRC Network [redacted].net
[redacted].hr
Your host is irc.[redacted], running version Unreal3.2.1
This server was created Sun Oct 17 2004 at 02:35:40 CDT
irc.[redacted] Unreal3.2.1 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeKVFNGCuzNT
WAP KNOCK SAFELIST HCN MAXCHANNELS=10 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307
MAXTARGETS=20 AWAYLEN=307 are supported by this server
[redacted] are supported by
this server
There are 1 users and 3815 invisible on 1 ser
101 unknown connection(s)
22 channels formed
I have 3816 clients and 0 servers
Current Local Users: 3816 Max: 5941
Current Global Users: 3816 Max: 4484
MOTD File is missing
Informações do Botnet

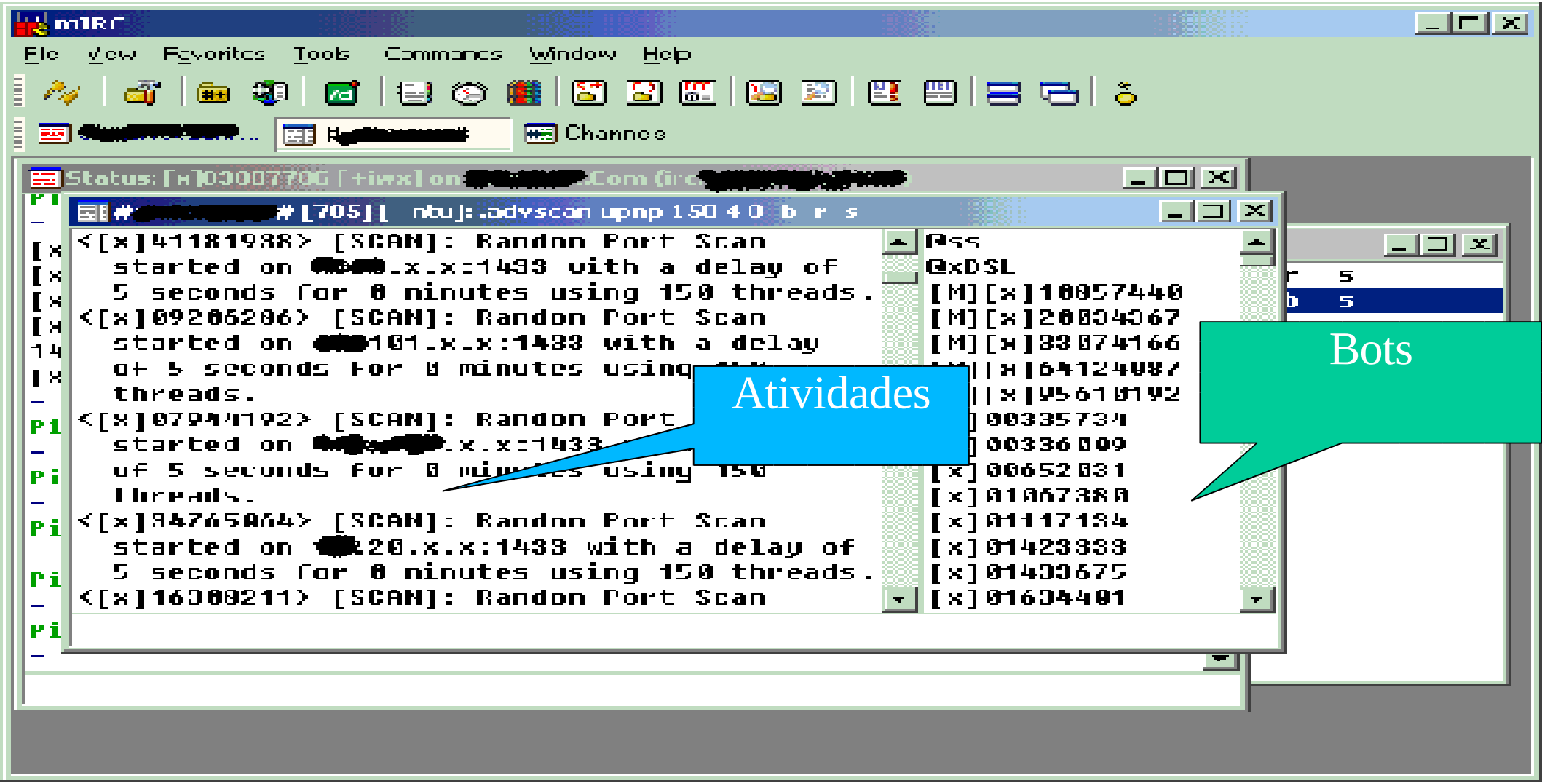
Botnets


mIRC
File View Favorites Tools Commands Window Help
Channels
513 [+ntl CnN] .advscan lsass_445 150 4 0 -b -r -s
2 [+ntl]
1 [+ntU]
* Now talking in #
* Topic is '.advscan lsass_445 150 4 0 -b -r -s '
* Set by xDSL on Thu Oct 21 22:09:28
* xDSL sets mode: +o xDSL
<xDSL> .l kill -s
<xDSL> .j #th
<xDSL> .l kill -s
<xDSL> .j #th
<xDSL> .l kill -s
<xDSL> .j #th
<xDSL> .l kill -s
<xDSL> .j #th
<xDSL> .l kill -s
<xDSL> .j #th
cc324512

RxBot – Base de 17 exploits!



Botnets



Botnets

[17:11] <randomnick> .up

[17:11] <[x]12212893> [MAIN]: Uptime: 1d 8h 50m.

[17:11] <[x]55483161> [MAIN]: Uptime: 2d 8h 18m.

[17:11] <[x]32705837> [MAIN]: Uptime: 2d 6h 49m.

[17:11] <[x]66729140> [MAIN]: Uptime: 0d 4h 2m.

[17:11] <[x]62694986> [MAIN]: Uptime: 0d 7h 0m.

[17:11] <[x]77045269> [MAIN]: Uptime: 23d 8h 10m.

[17:11] <[x]10568877> [MAIN]: Uptime: 0d 8h 8m.

[17:11] <[x]43332600> [MAIN]: Uptime: 0d 5h 8m.

[17:11] <[x]38093578> [MAIN]: Uptime: 0d 9h 14m.

[17:11] <[x]59464173> [MAIN]: Uptime: 29d 9h 14m.

[17:11] <[x]59968649> [MAIN]: Uptime: 23d 8h 9m.

[17:11] <[x]29780258> [MAIN]: Uptime: 0d 6h 29m.

[17:11] <[x]70324359> [MAIN]: Uptime: 23d 8h 10m.

Botnets

- Mas como detectar ?
  - Conhecendo seu inimigo!
    - Entender o funcionamento dos Bots
      - **Know your Enemy – Tracking Botnets**
    - Analises de Bots - LURHQ
      - http://www.lurhq.com/phatbot.html
    - Handlers Diaries no ISC (http://isc.sans.org)

Botnets

- Mas como detectar:
  - IDSs (canais, comandos...)
    - Como funciona um IRC (o que é um canal, modes, nicks, whois, list...)
    - Regras de ids para os comportamentos em canais
      - Snort chat.rules
      - Bleeding Snort Bot rules
    - Atenção as portas fora 6666:7000

!MoskeMongo.BIZ *** Listener on *:**59**, clients 11. is PERM
!MoskeMongo.BIZ *** Listener on *:**443**, clients 1145. is PERM
!MoskeMongo.BIZ *** Listener on *:6667, clients 133. is PERM

Combates a Bots e Botnets

- A verificação pode ser feita com qualquer cliente IRC (ex. mIRC)

- Alguns cuidados necessários:
  - Nunca verifique de dentro de sua empresa/orgão
    - Por que??
  - Alguns comandos podem ser retirados dos servidores (ex. /list)
    - Por que??

Combates e Bots e Botnets

- Tamanho não é Documento!
- O que vale mais:
  - Uma Botnet com 5000 máquinas ou uma com 1000 máquinas?
    - Parece obvio, mas não é!

Botnets

- Mas, e como reportar botnets ?

1) Contato com o ISP responsável

2) Através do Contact Form do ISC (http://isc.sans.org/contact.php)

- Envie informações completas sobre o Botnet
  - Qual o servidor
  - Qual o Canal
  - Senha do servidor/canal
  - AS do IP do Botnet (utilize o whois do Team Cymru, whois.cymru.com)
    - http://isc.sans.org/diary.php?date=2004-10-21

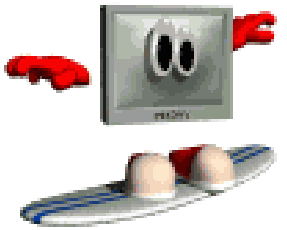
Combates a Bots e Botnets

- Você é responsável por algum AS?
  - Junte-se a NSP-SEC !
  - The nsp-security [NSP-SEC] forum is a volunteer incident response mailing list, which coordinates the interaction between ISPs and NSPs in near real-time and tracks exploits and compromised systems as well as mitigates the effects of those exploits on ISP networks. The list has helped mitigate attacks and will continue to do so.
    - https://puck.nether.net/mailman/listinfo/nsp-security
  - Conheça a **NSP-SEC-BR!** (em alguns instantes...)

Conclusões

- Os dias ingênuos da internet já se foram...
  - Antes:
    - 1 bot == $1 a $5 dólares ou 3 contas shell
  - Hoje
    - BotNets == $500 dolares
    - Ataques DDoS == $500 a $1500
    - ´Hackers for Hire'
  - Antes:
    - Script Kidz...
  - Hoje:
    - Crime Organizado!

Conclusão



Participe!

- Envie logs para o DShield

  (http://www.dshield.org/howto.php)
- Envie suas observações para o ISC

  (http://isc.sans.org/contact.php)
- Aprenda a fazer um hardening do seu sistema

  (http://www.sans.org)

pbueno@isc.sans.org / bueno@ieee.org

FIM