



SANS ISC

Bots e Botnets

Pedro Bueno, SANS GCIA

SANS Internet Storm Center

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



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

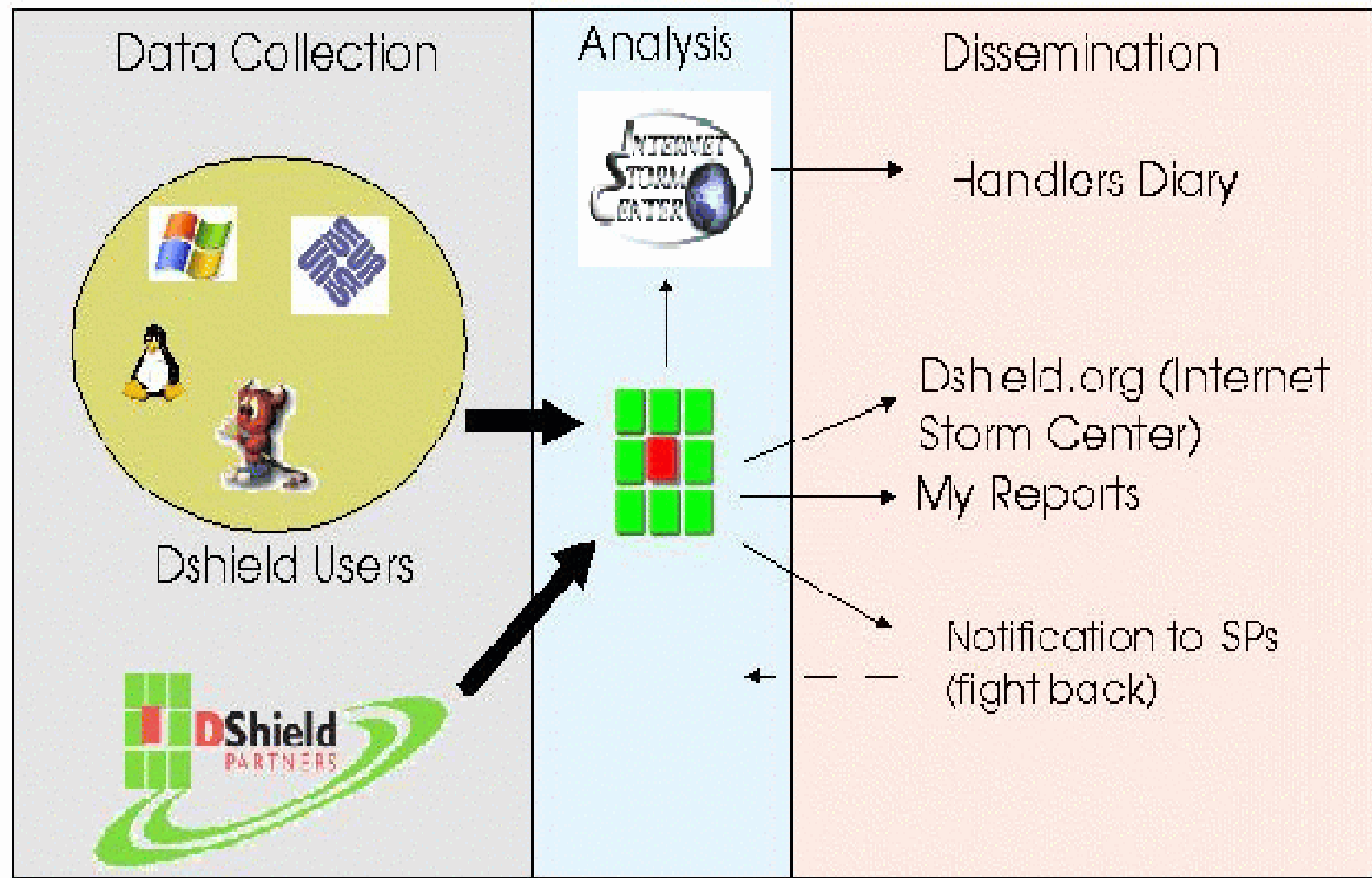
--Johannes Ullrich, CTO do SANS Internet Storm Center (ISC)

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!



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

The screenshot shows the ISC website interface. At the top, there are navigation links for 'SANS', 'SANS Home page', 'SANS Bankstars', 'SANS Reading Room', and 'SANS Portal'. Below this is a banner for 'SANS NETWORK SECURITY 2004 LAS VEGAS'. The main navigation bar includes 'Trends', 'Top 10', 'Reports', 'Contact', 'About', 'INFOCon', 'Presentations', and 'Links'. A sidebar on the left contains a search box, a 'Part I linkups' section with a 'GO' button, and a list of links: 'Part Graph', 'Part History', 'Today's Diary', 'Papers and Analysis', 'Survival Time', 'Database Statistics', 'Diary Archive', 'Trend History', 'ISSS News', and 'World Map'. The main content area features a 'Today's Diary' section with the title 'Ethics / SSH brute forcing continues'. The text in this section discusses the ethical implications of brute forcing SSH connections and mentions that the author generally calls such actions 'crackers' rather than 'hackers'. A 'World Map' section on the right displays a world map with pie charts indicating the geographical distribution of various security-related events or reports. Below the map is a 'Part History' section with a line graph showing trends over time.

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 notícias, dúvidas ou questionamentos aos handlers, utilize o formulário de contato(<http://isc.sans.org/contact.php>)



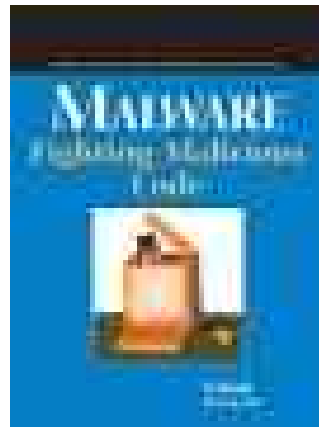
Malwares

- 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



- 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.

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

Update April 6, 2004

There are now over 700 variants of this Trojan-Dropper 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 PC Sdbot trojan was published on the Internet some time ago, and a number of worms are based on the same code. The following are some of the 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 (LEASS Vulnerability (CAN-2003-0333)). 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 * Aimbob * Alcobot * Babot *
Badbot * Bbot * Bigbot * Evilbot * Gobot * Msbot *
ShellBot * Psybot * Rbot * Sbot * Sdbot * Aebot *
GTBot * Nyrobot * Robobot * Rsbob * Vbbob * Padobot
* Kazabob * Gunbob * IRCBot ...

Caso Mytob = Mydoom + SdBot

The screenshot shows a web browser window displaying a news article. The article title is "Praga Mytob gera 95 variantes em 13 dias". The text discusses the rapid evolution of the Mytob malware, noting that it has generated 95 variants in just 13 days. It mentions that the malware is a combination of Mydoom and SdBot, and that it has been found to be particularly effective in spreading through email attachments. The article also includes a sidebar with a search bar, navigation links, and a list of related news items. The website has a yellow and black theme.

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.

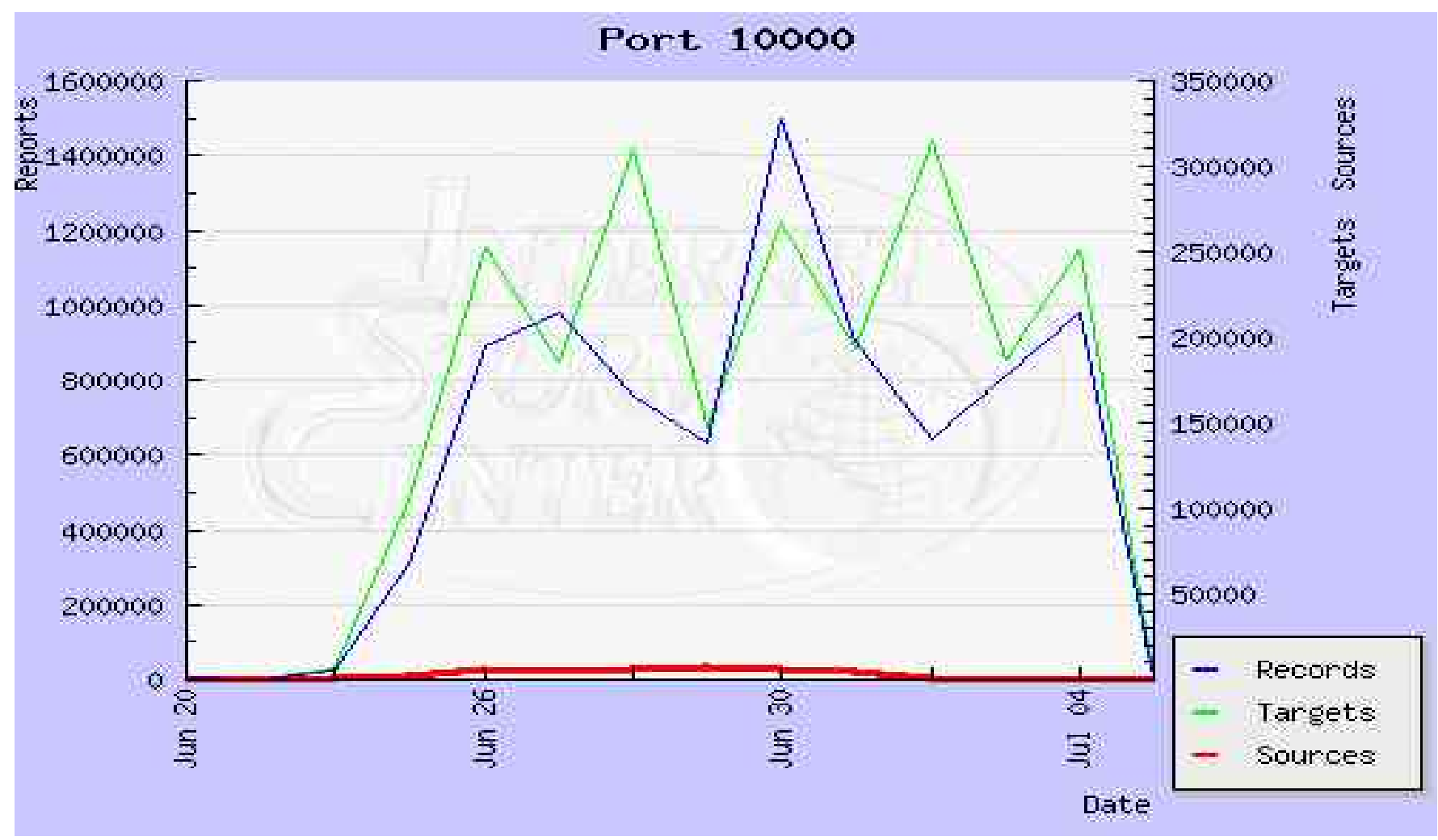
Regards,"

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.

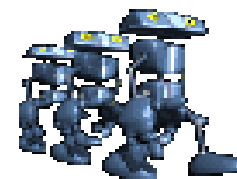
Malwares e o ISC

- 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!)

```

idos: Bloco de notas
Arquivo  Editor  Formatar  Exibir  Ajuda

/*
  Agobot's - a modular IRC bot for win32/linux
  Copyright (c) 2005 Agn

  This program is free software; you can redistribute it and/or
  modify it under the terms of the GNU General Public License
  as published by the Free Software Foundation; either version 2
  of the license, or (at your option) any later version.

  This program is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
  GNU General Public License for more details.

  You should have received a copy of the GNU General Public License
  along with this program; if not, write to the Free Software
  Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA. */

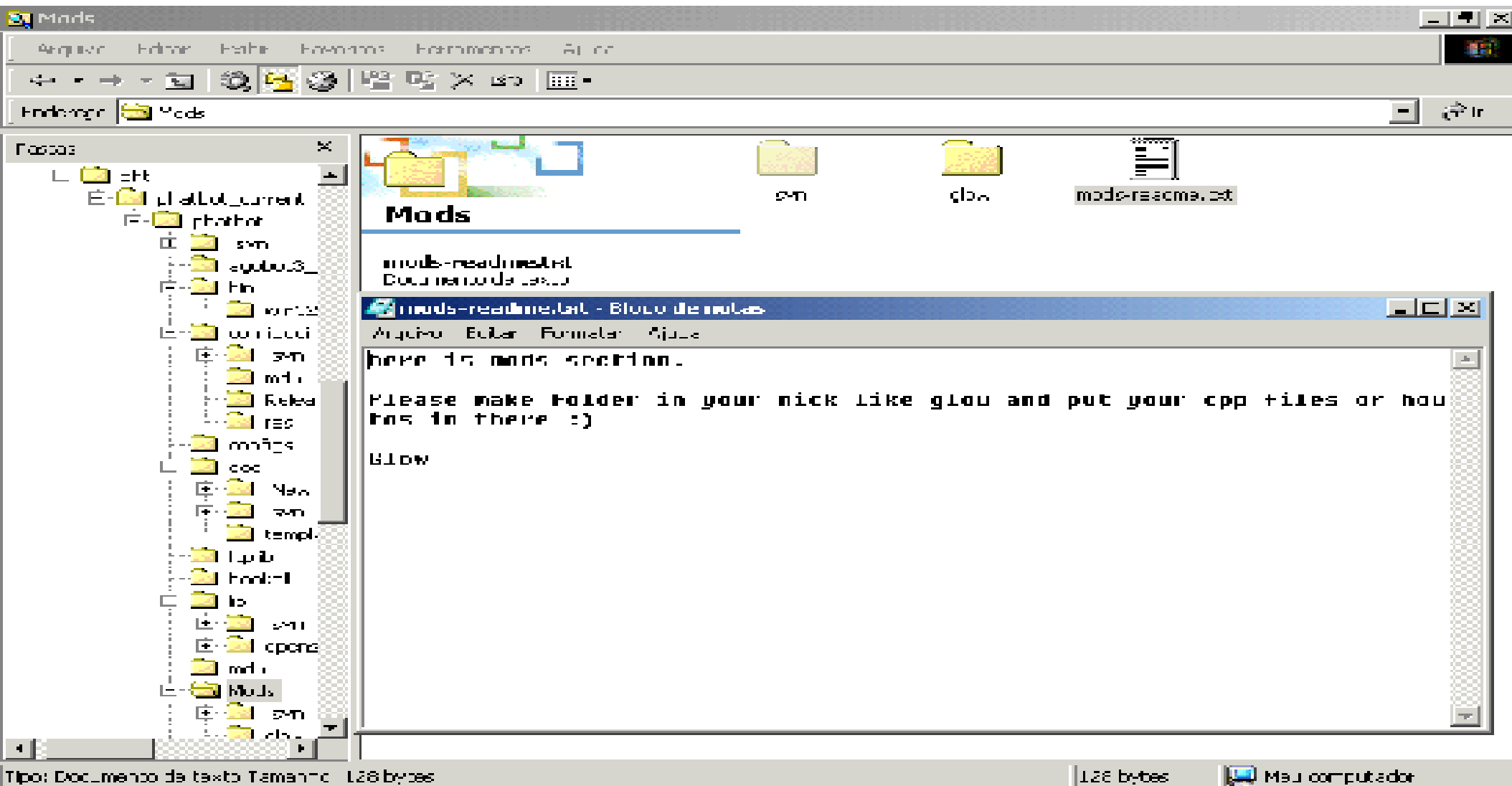
#include "main.h"
#include "cmds.h"
#include "mainnet.h"
#include "synflood.h"
#include "juniflood.h"
#include "ftppflood.h"

void CDDOS::Init()
{
  m_listen_hrcache=0; m_blocking=false;
  g_cmds[CMD_LISTEN].m_cmds.RegisterCommand(&CDDOS::m_blocking, "docs.pingflood",
  g_cmds[CMD_LISTEN].m_cmds.RegisterCommand(&CDDOS::m_blocking, "docs.ucpflood",
  g_cmds[CMD_LISTEN].m_cmds.RegisterCommand(&CDDOS::m_blocking, "docs.sppdflood",
  g_cmds[CMD_LISTEN].m_cmds.RegisterCommand(&CDDOS::m_blocking, "docs.synflood",
  g_cmds[CMD_LISTEN].m_cmds.RegisterCommand(&CDDOS::m_blocking, "docs.hrtflood",
  g_cmds[CMD_LISTEN].m_cmds.RegisterCommand(&CDDOS::m_blocking, "docs.sshd",

/*
  docs.synflood <host> <time> <delay> <count>
  = port 0 = random port
  docs.ucpflood <host> <number> <size> <delay> <count>
  = port 0 = random port
  
```

Criação de Malwares

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



Criação de Malwares

- Referência dos Comandos:

Agobot3
command reference
(for Agobot3 3.1.3 Alpha)

[Go to command reference](#) / [Go to help files](#) / [redircat](#) / [download](#)

command	alias	syntax	description	examples
Bot commands				
bot about		bot about	Displays the info the author wants you to see	Agobot3 bot about Agobot3: Agobot3 (3.1.3 Alpha) Release! "Ma32" by Agobot3 (Design@agobot3.com) / agobot3.com
bot die		bot die	terminates the bot	Agobot3 bot die Agobot3: Agobot3 has quit (read error: 101: connection reset by peer)
bot dns		bot dns <ip> <hostname>	execute ip to hostname or vice	Agobot3 bot dns agobot3.com Agobot3: agobot3.com host not found: 90: 0: 33 Agobot3 bot dns 90.0.0.33 Agobot3: 90.0.0.33 -> agobot3.com
bot execute		bot execute <command>	executes the bot execute command, use in hidden when visibility is 0, make the visibility and no effect on gui programs that dont have the visibility parameter (WebServer, etc)	Agobot3 bot execute C:\cmd.exe Agobot3: C:\cmd.exe (noepad.exe visible)

Criação de Malwares

- Modificação fácil do código fonte

The screenshot displays three Notepad++ windows containing C++ source code for malware development:

- dcomscanner.cpp**: Shows the beginning of a class `CScannerDCOM` that inherits from `CScannerBase`. It includes headers `main.h`, `mainctrl.h`, `utility.h`, and `shellcode.h`.
- baglescanner.cpp**: Shows the beginning of a class `CScannerBagle` that inherits from `CScannerDCOM`. It includes headers `main.h`, `mainctrl.h`, and `utility.h`.
- ddos.cpp**: Shows the `Init()` method of the `CDDOS` class. It registers several flood types:
 - `REGCMD(n_cmdUDP, "ddos.udp", false, this);` - "starts udp flood"
 - `REGCMD(n_cmdSyn, "ddos.syn", false, this);` - "starts syn flood"
 - `REGCMD(n_cmdHTTP, "ddos.http", false, this);` - "starts http flood"
 - `REGCMD(n_cmdStop, "ddos.stop", false, false);` - "stops all floods"
 - `REGCMD(n_cmdPhatSyn, "ddos.phatsyn", false, this);` - "starts syn Flood"
 - `REGCMD(n_cmdPhatICMP, "ddos.phaticmp", false, this);` - "starts icmp Flood"

Criação de Malwares

Nome	Tipo	Modificado	Tamanho	Caract.	Exibido	Nome	Tamanho
anti-bulk-headers	ARCHIVE File	22/3/2004 17:05	4	1.6		photocon...	
cockerconnection.op.en-base	SQL BSAFE File	22/3/2004 17:23	1	0.0		photocon...	
download-over-time	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	
download-over-time	ARCHIVE File	21/3/2004 17:25	4	1.6		photocon...	
evoker.app.en-base	ARCHIVE File	22/3/2004 17:05	4	1.6		photocon...	
evoker.h.en-base	SQL BSAFE File	21/3/2004 17:23	1	0.0		photocon...	
evoker.h.en-base	SQL BSAFE File	21/3/2004 17:25	30	0.0		photocon...	
evoker.h.en-base	ARCHIVE File	21/3/2004 17:25	4	1.6		photocon...	
edward.op.en-base	ARCHIVE File	22/3/2004 17:05	4	1.6		photocon...	
edward.h.en-base	SQL BSAFE File	21/3/2004 17:23	1	0.0		photocon...	
evoker.en-base	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	
evoker.en-base	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
doorzscammer.op.en-base	ARCHIVE File	22/3/2004 17:05	4	1.6		photocon...	
doorzscammer.op.en-base	SQL BSAFE File	21/3/2004 17:23	1	0.0		photocon...	
download-over-time	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	
download-over-time	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
debug.op.en-base	ARCHIVE File	22/3/2004 17:05	4	1.6		photocon...	
disclaimer.en-base	SQL BSAFE File	21/3/2004 17:23	1	0.0		photocon...	
download-over-time	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	
kernel.en-base	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	ARCHIVE File	22/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:23	1	0.0		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	
kernel.en-base	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:23	1	0.0		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	
kernel.en-base	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:23	1	0.0		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	
kernel.en-base	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	ARCHIVE File	21/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:23	1	0.0		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	
kernel.en-base	ARCHIVE File	22/3/2004 17:05	4	1.6		photocon...	
kernel.en-base	SQL BSAFE File	22/3/2004 17:05	1	0.0		photocon...	
kernel.en-base	SQL BSAFE File	21/3/2004 17:25	1	0.0		photocon...	

Selected 6 files, 0 bytes Total 22.8K files, 100.4K total



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

PhantomPAG - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.ghostscript.com/ghostscript/faq/faqFAQ04.html

Content Advisor: 12/15/2006 12:15:00 PM

[L.5] How to use agobot3

Because this tool is GPL, you can't have a "version" and unless of the "current" version 3 or 4 of the "supported" version, if I don't, you can't still try and compile, but you should consider notifying me so I can update my documentation. I'm always looking for people who test my bot on Linux flavors I didn't test it on.

edit: Make file to enable optimization or debug, you just have to remove some # signs to uncomment the lines. After this type "make", it will start compilation, and if everything works well you will end up with an agobot3 executable that you can test using "agobot3" if you're using "make".

events that the bot does on Linux. It's not a bot, but it mostly works at least in install on Linux if you try to "exec" startup at the moment, but I'm planning on fixing this in reasonable time.

[L.6] Which systems are tested?

Debian 3.0	2.4.20-3-k2	gcc / gcc version 3.3.1 / 38704 (Ubuntu 3.3.1-1)
Debian 3.0	2.4.20	gcc / gcc version 3.2.2
FreeBSD 5.3	???	gcc / gcc version 3.3.1 / 2000722 (Debian 3.3.1-1) / compiled in Debian
FreeBSD 5.1	2.4.21	gcc / gcc version 3.2
Windows 2003 Server English	SP4	visual C++ 6.0 6.0 SP5
Windows 2003 Server English	SP3	visual C++ 6.0 6.0 SP5
Windows 2003 Sp4 English	SP4	visual C++ 6.0 6.0 SP5
Windows 2003 Pro English	SP3	visual C++ 6.0 6.0 SP5
Windows 2003 Sp4 German	SP	visual C++ 6.0 6.0 SP5
Windows 2003 Server English	SP0	visual C++ 6.0 6.0 SP5
Windows 2003 Server English	SP	visual C++ 6.0 6.0 SP5
Windows XP Pro English	SP0	visual C++ 6.0 6.0 SP5

Done

Criação de Malwares

FAQ!

The screenshot shows the 'Agobot Config GUI' window. On the left, a list of configuration parameters is shown, with 'cdos_maxthreads' selected. Below this list are buttons for 'Add Server', 'Delete Server', and checkboxes for 'Test Server' and 'Use CG...'. A list box contains 'New1'. Below the list box are input fields for 'Server', 'Server Password', 'Main Channel', 'Channel Password', and 'Nick Prefix'. A blue callout bubble points to the 'Server' field with the text 'Parâmetros do server'. On the right, there are buttons for 'Edit Script', 'FAQ', and 'Cmd Ref'. Below these are 'Properties' and 'Value' sections. A text area contains the sentence 'A kind of Darwinism pervades the world of nejan net development'. Below this are 'Add User' and 'Delete User' buttons, and another 'New' list box. Below the list box are input fields for 'Username', 'Password', 'Hostmask', and 'Identmask'. At the bottom right, there are input fields for 'Payment Section Name' (containing 'www.isc.org') and 'Key Length' (containing '16'). A blue callout bubble points to the 'Username' field with the text 'Parâmetros do Usuário'.

Criação de Malwares

The screenshot shows the Agobot Config GUI with the following details:

- Buttons:** Generate Config, Cancel, Load from, Save to, Edit Script, Add, Find Port, Add Server, Delete Server, Add User, Delete User.
- Properties List:**
 - main_channel - String
 - inst_polymorph - Boolean
 - scaninfo_channel - String
 - scaninfo_interval - Integer
 - scaninfo_enabled - Boolean
 - spam_col_enabled - Boolean
 - spam_col_channel - String
 - scaninfo_level - Integer
 - odken_windows - Boolean
 - ident_name - Boolean
 - red_maxthreads - Integer
 - ddos_maxthreads - Integer
- Server List:**
 - ed[redacted].com:8080 - #channel
 - [redacted].com:8080 - #channel
- User List:**
 - ghct0 - User2
- Form Fields:**
 - Server: ed[redacted].com
 - Server Password: [empty]
 - Main Channel: #channel
 - Channel Password: 23phat
 - Nick Prefix: pB-
 - Username: ghct0
 - Password: null
 - Hostmask: [empty]
 - Identmask: User2
 - Polymorph Section Name: [empty]
 - Sec Length: 16

Repositórios de Bots

The screenshot shows a web browser window displaying an index of files and folders. The browser's address bar shows a URL starting with 'http://'. The page title is 'Index of [redacted]'. Below the title is a table with columns for Name, Last modified, Size, and Description. The table lists several folders, including 'botnet', 'botnet2', 'botnet3', 'botnet4', 'botnet5', 'botnet6', 'botnet7', 'botnet8', and 'botnet9'. The 'Last modified' column shows dates ranging from 01 May 2005 to 04 May 2005. The 'Size' column shows values like 10:34, 19:30, 10:35, 19:34, 10:35, 19:31, and 19:34. At the bottom of the page, it says 'Apache/2.2.3 Server at [redacted] Port 80'.

Name	Last modified	Size	Description
botnet	01 May 2005 10:34	10:34	
botnet2	01 May 2005 19:30	19:30	
botnet3	01 May 2005 10:35	10:35	
botnet4	04 May 2005 19:34	19:34	
botnet5	01 May 2005 10:35	10:35	
botnet6	04 May 2005 19:31	19:31	
botnet7	01 May 2005 10:35	10:35	
botnet8	04 May 2005 19:34	19:34	

Repositório de Bots

Index of [redacted]

Name	Last Modified	Size	Content Type
Parent Directory	09-Sep-2005 19:00	-	-
aghost/	09-Sep-2005 10:38	-	-
black/	09-Sep-2005 19:00	-	-
gpc/	09-Sep-2005 19:00	-	-
modsp/	09-Sep-2005 10:38	-	-
misp/	14-Sep-05 19:00	-	-
rbcc/	09-Sep-2005 19:00	-	-
smb/	09-Sep-2005 10:38	-	-
smb2/	14-Sep-05 19:00	-	-
w32pc/	09-Sep-2005 19:00	-	-
w32pc2/	09-Sep-2005 10:38	-	-
w32pc3/	09-Sep-2005 19:00	-	-

Apresentamos 12 arquivos e 12 subdiretórios. [redacted] (total de 12)

E não é só isso...



Bots em perl...

- O Brasil é um dos líderes 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.xxxxxxxxxxxx.net

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

xxx.xxxxxxxxxxxx.org

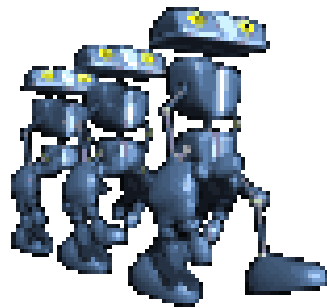
Regards, xxxx@xxxxxx

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

- Simple:
 - 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!?”™

```
mTRC - [Status: [-_]22340 [-ix] on [redacted] (irc.[redacted].com)]
File View Favorites Tools Commands Window Help
irc.[redacted].com [redacted] 223... 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]!x3245126[redacted]-081-810.[redacted].net
.br
Your host is irc.[redacted].com, running version Unreal3.2.1
This server was created Sun Oct 17 2004 at 02:35:40 CDT
irc.[redacted].com Unreal3.2.1 loughraAsDRTVsxNcUqBzvdHtGp 1vhopsmtikrRcaqQALQbSeKVFNGCuzNT
MAP KNOCK SAFELIST HCN MAXCHANNELS=10 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307
MAXTARGETS=20 AWAYLEN=307 are supported by this server
MAXCHANNELS=128 SILENCE=15 MINS=12 CHANNELS=# PREFIX=(qao)~* CUANMIN S=he,kll,l,psmti
PRDUNQKUGCuzNSMI NETWORK=[redacted] CASEMAPPING=ascii EXIBON=",cqr ELISI-MNUCI 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: 4684
NOTD File is missing
```

Informações do Botnet

Botnets

The screenshot shows an IRC client window with a menu bar (File, View, Favorites, Links, Commands, Window, Help) and a toolbar. The main window displays a list of channels:

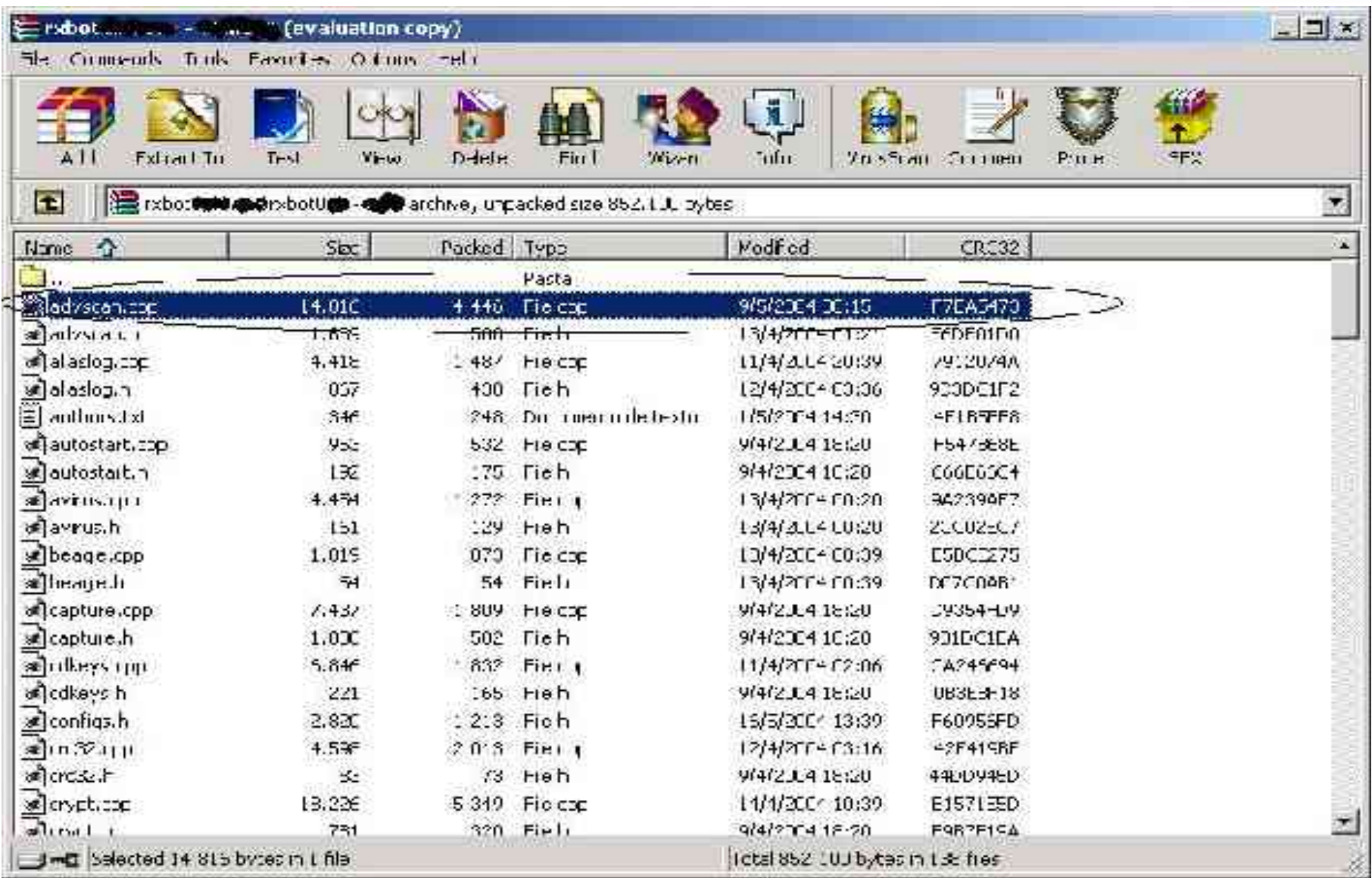
Channel Name	Mode	Topic
513	[+smulGN]	.advscan 1sass_445 150 4 0 -b -r -s
2	[+ntL]	
1	[+ntU]	

A blue arrow points to the channel with 2 members. A smaller window below shows the details for this channel:

```
# [1] [-lmnStu]: .advscan 1sass_445 150 4 0 -b -r -s  
* Now talking in #  
* Topic is '.advscan 1sass_445 150 4 0 -b -r -s'  
* Set by xDSL on Thu Oct 21 22:09:20  
* 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
```

The right side of the channel window shows the user ID `cc824512`.

RxBot – Base de 17 exploits!



Botnets

The screenshot shows an IRC window with a channel named # [705]. The main window displays a list of bots and their activities. A blue callout box labeled "Atividades" points to the scan messages, and a green callout box labeled "Bots" points to the bot list.

```
Status: [x]03007700 [+iwx] on [redacted].Com (irc.[redacted].com)
# [redacted] # [705] [ntu]:.advyscan upnp 150 40 b r s
<[x]41181988> [SCAN]: Randon Port Scan
started on [redacted].x.x:1433 with a delay of
5 seconds for 0 minutes using 150 threads.
<[x]09206206> [SCAN]: Randon Port Scan
started on [redacted]101.x.x:1433 with a delay
of 5 seconds for 0 minutes using 150
threads.
<[x]07944102> [SCAN]: Randon Port
started on [redacted].x.x:1433
of 5 seconds for 0 minutes using 150
threads.
<[x]84765064> [SCAN]: Randon Port Scan
started on [redacted]20.x.x:1433 with a delay of
5 seconds for 0 minutes using 150 threads.
<[x]16000211> [SCAN]: Randon Port Scan
Ass
@xDSL
[M] [x]10057440
[M] [x]20004067
[M] [x]33074166
[M] [x]64124087
[M] [x]95610192
00335734
00336009
[x] 00652031
[x] 01067380
[x] 01117134
[x] 01423333
[x] 01400675
[x] 01604401
```

[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.

- 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>)



- 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...

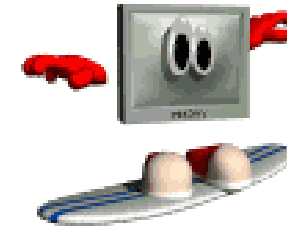
- Hoje:

- 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

