



# SANS ISC

## Formas de Combates a 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)

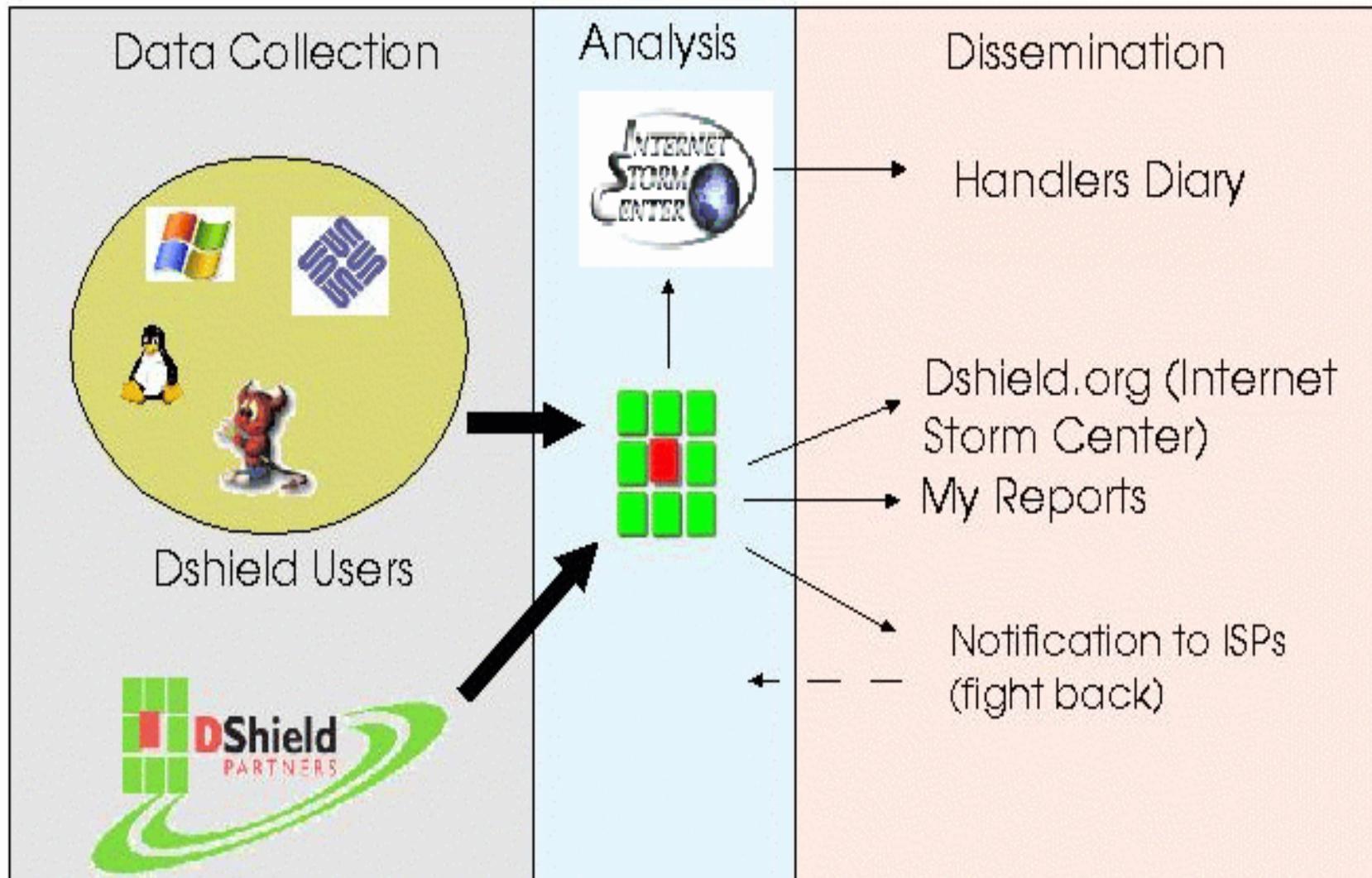
# Agenda

---

- Introdução ao ISC
  - Sensores Distribuídos e DShield.org
  - Analise dos Dados e a Lista dos Handlers
- Estudo da nova tendência de criação de Malwares
  - Slammer Worm
  - Sasser Worm
  - AGO/GAO/PhatBot Variantes
- Bot e Botnets
- Conclusões



# 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

SANS
SANS Homepage
SANS Bookstore
SANS Reading Room
SANS Portal

InfoCon: **GREEN**

**SANS NETWORK SECURITY 2004**  
 Sep. 28-Oct. 04 Register Now!

Handler on Duty: Patrick Nolan 19:39:52 UTC Sep 12 2004 15:39:52 Sep 12 2004

Trends Top 10 Reports Contact About INFOCon Presentations Links XML

Handler's Diary: Ethics / SSH brute forcing continues

**Port Lookup:**  
80

- + Port Graph
- Port History
- Today's Diary
- + Papers and Analysis
- Survival Time
- + Database Statistics
- + Diary Archive
- + Trend History
- + ISTS News
- World Map

[Learn how to include the InfoCon logo on your homepage](#)

## Today's Diary

Previous

**Handlers Diary September 11th 2004**

Updated September 11th 2004 23:36 UTC (Handler: Swa Frantzen)

**Ethics / SSH brute forcing continues**

On a day like this it's not such a big effort to ponder about the different mentality and ethics people have. Don't worry, I won't go away from the information security scene.

**Ethics**

Crackers

I generally call people breaking into systems crackers, not hackers.

Why do they do it? Because they can.

Do they know they cause a lot of work? Yes: they will often try to minimize the work by leaving the original content in a backup copy.

In their ethical view it's right, all you need to do as a defender is fix the bug and reinstall the backup over their defacement. Unfortunately this is only true is you know 100% sure the cracker didn't do anything else, otherwise it takes a lot more work.

Spammers

## World Map

■ microsoft-ds,445	■ epmap,135	■ dabber,9898
■ sasser-ftp,5554	■ netbios-ns,137	■ Reserved,10
■ other	Sep 10th 2004	

## Port History

--- 445
--- 135
--- 9898
--- 137
--- 5554

# 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

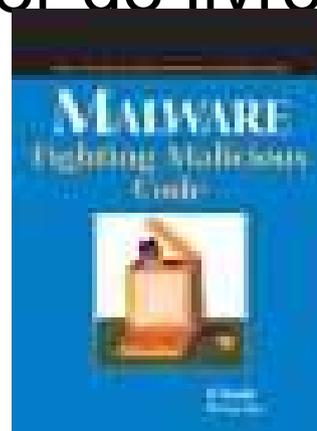
---

- 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



# Malwares

- Por que estamos vendo uma onda de Malwares em 2004?
  - Em abril, 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.

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

-- Update April 6, 2004 --

There are now over 700 variants of this trojan-turned 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 some examples of such worms:

- W32/Sdbot.worm
- W32/Sdbot.worm.gen
- W32/Sdbot.worm.gen.b

•50 variantes por semana

## Large Numbers of Gaobot Worm Variants Proliferating

April 29, 2004

McAfee Thursday issued an alert for W32/Gaobot.worm.ali, 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.ali 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.

# Detecção da Evolução dos Malwares

---

- Fluxo normal na criação de Worms
  - Publicação da Vulnerabilidade
    - Com ou sem correção por parte do fabricante
    - Ultimamente coordenado com o fabricante
  - Implementação dos PoC (Proof-of-Concept) distribuídos publicamente
    - Websites (K-otik ??) , Listas de Discussão (Full-Disclosure ??)
    - Boa parte restrito ao underground (moeda de troca!)
  - Automatização dos Exploits
    - 3 passos
      - Scanning
      - Comprometimento
      - Ações Maliciosas (Backdoors, DDoS...)

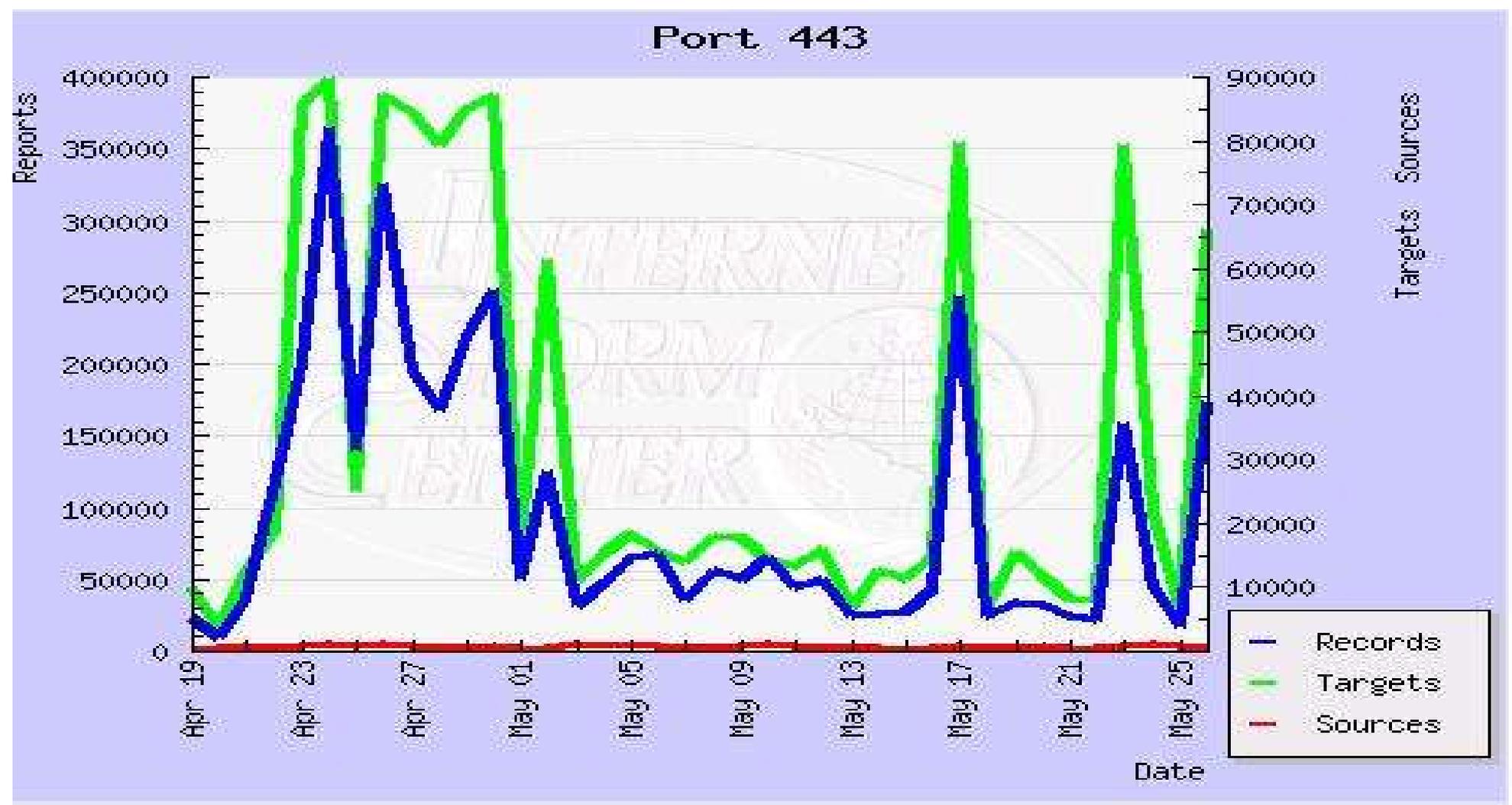
# Malwares e o ISC

---

- Detecção de Worms
  - 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.

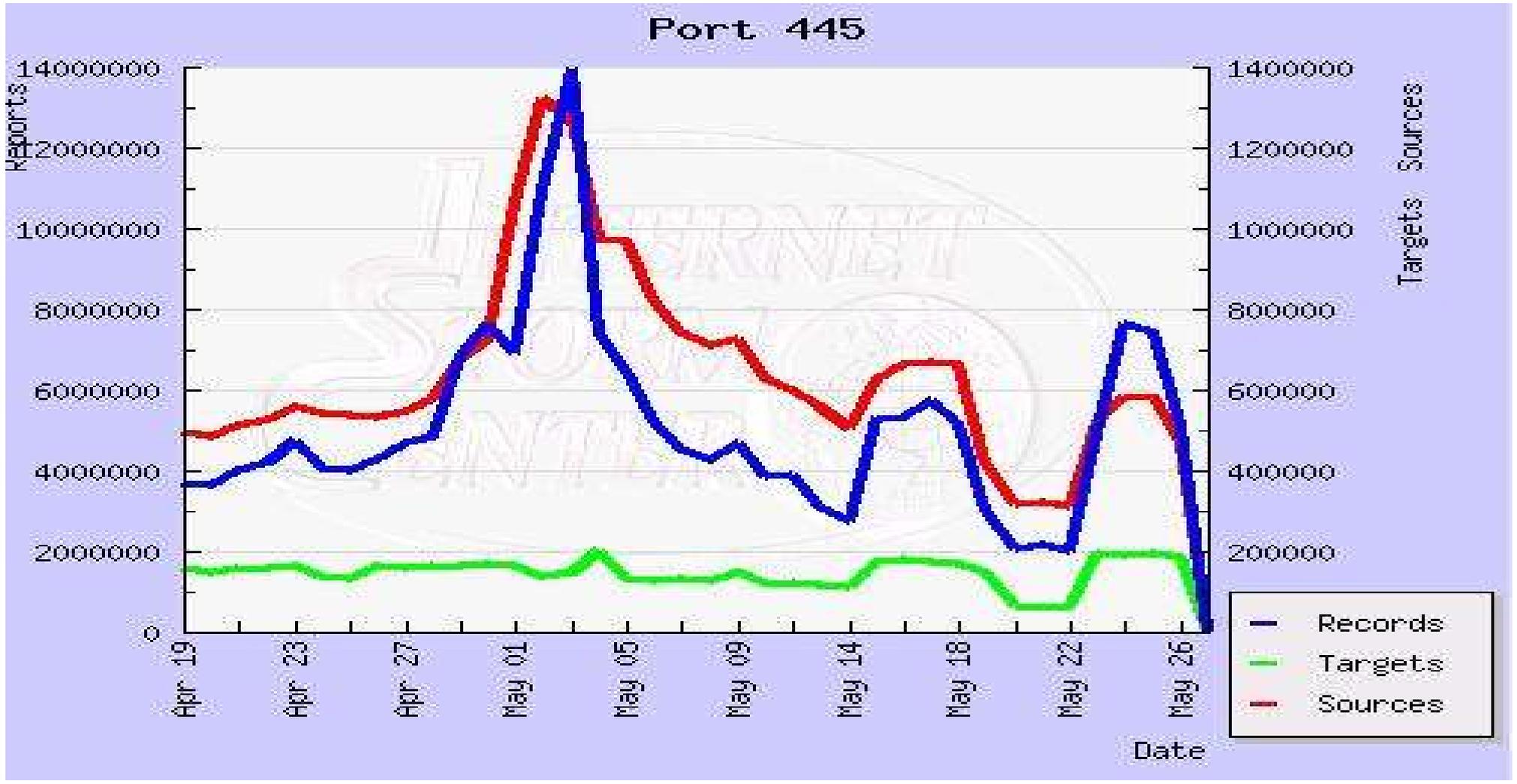
# Malwares e o ISC

- Exemplo 1: Porta 443 – Tráfego sem worm



# Malwares e o ISC

- Exemplo 2: Porta 445 – alta probabilidade de worm



# Criação de Malwares

- Caso 1: Slammer Worm



25 de Julho de 2002: Microsoft Security Bulletin MS02-39 – vulnerabilidade no MS-SQL Server

- Novembro de 2002: Website PacketstormSecurity publica o primeiro exploit
- 24/25 de Janeiro de 2003: Slammer Day!

**Tempo de desenvolvimento: 6 meses!**

# Criação de Malwares

- Caso 2: Sasser Worm – Abril 2004

11	12	13 Patch Day	14 IIS DOS exploit	15 LSASS exploit	16	17	< 2 weeks to patch !
18	19	20 TCP RST	21 IIS SSL exploit	22	23	24	< 3 weeks to worm
25 public LSASS exploit	26	27 LSASS Gaobot	28	29 MSFT Patch Errata	30 <b>SASSER</b>	1 May sasser.b	
2 May sasser.c	3 sasser.d	4	5	6	7	8	(e/f on May 9th)

Tempo de desenvolvimento: 17 dias

# Criação de Malwares

---

- Mydoom.AI – descoberto em 08 de Novembro de 2004
  1. Chega em emails (header informa que foi scaneado contra virus);
  2. Não carrega o vírus;
  3. Fornece um link com uma noticia interessante (Pr0n) para que o usuário clique;
  4. A página faz uso de uma vulnerabilidade IFRAME no IE (que NÃO há patch!) para infectar o computador remoto ;

**Vulnerabilidade pública em 2 de Novembro de 2004**

**Tempo de Desenvolvimento: 6 Dias!**

---

# Criação de Malwares

---

- Bots!
- Software que realiza ações em nome de um humano
- Não muita diferença dos worms
- Permite um controle remoto da máquina através de IRC (Internet Relay Chat), p2p...
- Vários propósitos:
  - DDoS
  - Relay para Spam
  - Proxy Anônimo
  - Controle total da máquina via IRC
- Vários bots sob o domínio 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

---

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

# Criação de Malwares

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

```

ddos - Bloco de notas
Arquivo  Editar  Formatar  Exibir  Ajuda
/*
  Agobot3 - a modular IRC bot for win32/Linux
  Copyright (C) 2003 Ago

  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. */

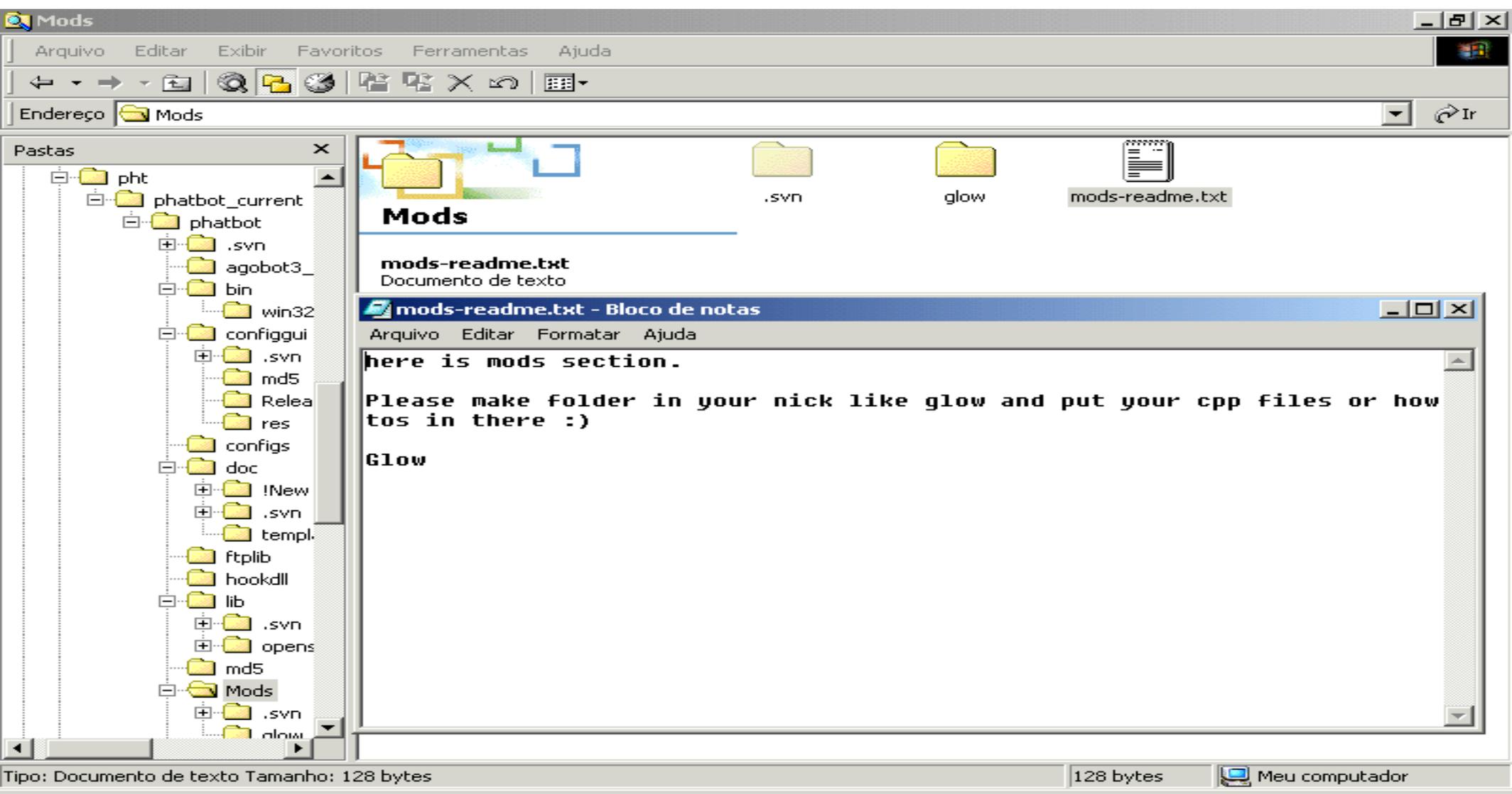
#include "main.h"
#include "ddos.h"
#include "mainctrl.h"
#include "synflood.h"
#include "junoflood.h"
#include "httpflood.h"

void CDDOS::init()
{
    m_iNumThreads=0; m_bDDOSing=false;
    g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdPing,           "ddos.pingflood",           ""
    g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdUDP,           "ddos.udpflood",           ""
    g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdSpooferUDP,     "ddos.spudpflood",        ""
    g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdSyn,           "ddos.synflood",          ""
    g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdHTTP,          "ddos.httpflood",         ""
    g_cMainCtrl.m_cCommands.RegisterCommand(&m_cmdStop,          "ddos.stop",              ""

/*
  .ddos.synflood <host> <time> <delay> <port>
  - port 0 = random port
  .ddos.udpflood <host> <number> <size> <delay> <port>
  - port 0 = random port
  
```

# Criação de Malwares

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



The screenshot shows a Windows XP file explorer window titled 'Mods'. The address bar shows the path 'Endereço Mods'. The left pane shows a tree view of folders, including 'pht', 'phatbot\_current', 'phatbot', and 'Mods'. The main pane shows the contents of the 'Mods' folder: a folder named '.svn', a folder named 'glow', and a text file named 'mods-readme.txt'. An open Notepad window titled 'mods-readme.txt - Bloco de notas' is overlaid on the main pane, showing the following text:

```

here is mods section.

Please make folder in your nick like glow and put your cpp files or how
tos in there :)

Glow
  
```

The status bar at the bottom of the Notepad window indicates 'Tipo: Documento de texto Tamanho: 128 bytes' and '128 bytes Meu computador'.

# Criação de Malwares

- Referência dos Comandos:



The screenshot shows a Mozilla Firefox browser window with the title "agobot3 command reference - Mozilla Firefox". The address bar shows the file path: "file:///C:/Documents%20and%20Settings/pedro/Desktop/iccyber/agobot/agobot3-priv/doc/commandref.html". The main content area displays the "Agobot3 command reference" document, which includes a table of bot commands.

command	alias	syntax	description	example
<b>bot commands</b> <span style="float: right;"><a href="#">top</a></span>				
bot.about		bot.about	displays the info the author wants you to see	<Ago> .bot.about <Agobot3> Agobot3 (0.1.3 Alpha) "Release" on "Win32" by Ago (theago@gmx.net): homepage: http://none.yet/
bot.die		bot.die	terminates the bot	<Ago> .bot.die <-- Agobot3 has quit (Read error: 104 (Connection reset by peer))
bot.dns		bot.dns <hostname/ip>	resolves ip/hostname by dns	<Ago> .bot.dns ago.bastart.net <Agobot3> ago.bastart.net -> 90.0.1.55 <Ago> .bot.dns 90.0.1.55 <Agobot3> 90.0.1.55 -> ago.bastart.net
bot.execute		bot.execute <visibility> "<command>"	makes the bot execute an .exe, exe is hidden when visibility is 0. note that visibility has no effect on gui programs that dont honor the visibility parameter WinMain gets.	<Ago> .bot.execute 1 notepad.exe (Victim executes notepad.exe visible)

Done

# Criação de Malwares

- Modificação fácil do código fonte

The screenshot displays three Notepad++ windows on a Windows XP desktop. The top window, titled 'dcomscanner.cpp - Bloco de notas', contains the following code:

```
#include "main.h"
#include "mainctrl.h"
#include "utility.h"
#include "shellcode.h"

class CScannerDCOM : public CScannerBase
{
public:
    CScannerDCOM();
    virtual ~CScannerDCOM();
    virtual void Init();
    virtual void Run();
};
```

The middle window, titled 'baglescanner.cpp - Bloco de notas', contains the following code:

```
/*$T baglescanner.cpp GC
/*$6
*****
*****
*****
*****
*/

#include "main.h"
#include "mainctrl.h"
#include "utility.h"

class CScannerBagle :
public CScannerBase
```

The bottom window, titled 'ddos.cpp - Bloco de notas', contains the following code:

```
#include "main.h"
#include "mainctrl.h"
#include "ddos.h"

void CDDOS::Init()
{
    m_iNumThreads=0; m_bDDOSing=false;
    REGCMD(m_cmdUDP, "ddos.udpflood", "starts
a UDP flood", false, this);
    REGCMD(m_cmdSyn, "ddos.synflood", "starts
an SYN flood", false, this);
    REGCMD(m_cmdHTTP, "ddos.httpflood", "starts
a HTTP flood", false, this);
    REGCMD(m_cmdStop, "ddos.stop", "stops
all floods", false,
this);
    REGCMD(m_cmdPhatSyn, "ddos.phatsyn", "starts syn
flood", false, this);
    REGCMD(m_cmdPhatICMP, "ddos.phaticmp", "starts icmp
```

# 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

WinZip (Evaluation Version) - phatbot\_source.zip

File Actions Options Help

New Open Favorites Add Extract Encrypt View CheckOut Wizard

Name	Type	Modified	Size	Ratio	Packed	Path
contrib.txt.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
cpanelscanner.cpp.svn-base	SVN-BASE File	22/3/2004 16:39	4	0%	4	phatbot_curre...
cplugin.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
cplugin.h.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
crypter.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
crypter.h.svn-base	SVN-BASE File	21/3/2004 17:22	4	0%	4	phatbot_curre...
cstring.cpp.svn-base	SVN-BASE File	21/3/2004 17:22	30	0%	30	phatbot_curre...
cstring.h.svn-base	SVN-BASE File	21/3/2004 17:23	30	0%	30	phatbot_curre...
cthread.cpp.svn-base	SVN-BASE File	22/3/2004 16:39	4	0%	4	phatbot_curre...
cthread.h.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
cvar.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
cvar.h.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
dcom2scanner.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
dcomscanner.cpp.svn-base	SVN-BASE File	21/3/2004 17:22	4	0%	4	phatbot_curre...
ddos.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
ddos.h.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
debug.sh.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
disclaimer.txt.svn-base	SVN-BASE File	21/3/2004 17:22	4	0%	4	phatbot_curre...
doomscanner.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
dwscanner.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
files.txt.svn-base	SVN-BASE File	22/3/2004 16:39	30	0%	30	phatbot_curre...
gpl.txt.svn-base	SVN-BASE File	21/3/2004 17:22	4	0%	4	phatbot_curre...
harvest_aol.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
harvest_aol.h.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
harvest_cdkeys.cpp.svn-base	SVN-BASE File	22/3/2004 16:39	4	0%	4	phatbot_curre...
harvest_cdkeys.h.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
harvest_emails.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
harvest_emails.h.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
harvest_registry.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
harvest_registry.h.svn-base	SVN-BASE File	21/3/2004 17:22	4	0%	4	phatbot_curre...
hook.cpp.svn-base	SVN-BASE File	21/3/2004 17:22	4	0%	4	phatbot_curre...
hook.h.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
httpflood.cpp.svn-base	SVN-BASE File	21/3/2004 17:23	4	0%	4	phatbot_curre...
installer.cpp.svn-base	SVN-BASE File	22/3/2004 16:39	4	0%	4	phatbot_curre...
installer.h.svn-base	SVN-BASE File	21/3/2004 17:22	4	0%	4	phatbot_curre...

Selected 0 files, 0 bytes      Total 1295 files, 184.958KB



# Criação de Malwares

---

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

# Criação de Malwares

PhatBot:FAQ - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

file:///C:/phatsrc/phatbot\_current/phatbot/doc/!New/FAQ.htm

Getting Started Latest Headlines

[1.5] How to use GCC ?

Execute this:  
`gcc -v 2>&1 | grep "gcc version"`  
 and check if the reported version is one of the supported version, if it isn't, you can 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 Makefile to enable optimization or debug, you just have to remove some # signs to uncomment the line. 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 bash.  
 Beware that the Linux version isn't a finished bot, but it mostly works. It has no installer to add itself to SysV startup at the moment, but I'm planning on fixing this in reasonable time.

[1.6] Which systems are tested ?

Debian 3.0	2.4.20-3-k6	libc6 / gcc version 3.3.1 20030728 (Debian prerelease)
Slackware 9.0	2.4.20	libc6 / gcc version 3.2.2
FreeBSD 4.8	???	libc6 / gcc version 3.3.1 20030728 (Debian prerelease) / compiled in debian
SuSe 8.1	2.4.21	libc6 / gcc version 3.2
Windows 2000 Server English	SP4	Visual Studio 6.0 SP5
Windows 2000 Server English	SP3	Visual Studio 6.0 SP5
Windows 2000 Pro English	SP4	Visual Studio 6.0 SP5
Windows 2000 Pro English	SP3	Visual Studio 6.0 SP5
Windows 2000 Pro German	SP1	Visual Studio 6.0 SP5
Windows 2003 Server English	SP0	Visual Studio 6.0 SP5
Windows 2003 Server English	SP1	Visual Studio 6.0 SP5
Windows XP Pro English	SP0	Visual Studio 6.0 SP5

Done

# Criação de Malwares

**FAQ!**

The screenshot shows the Agobot Config GUI with several annotations. A blue arrow points to the 'ddos\_maxthreads' parameter in the list. A blue speech bubble labeled 'Parâmetros do server' points to the 'Server' field in the configuration form. Another blue speech bubble labeled 'Parâmetros do Usuário' points to the 'Username' field in the configuration form. The 'FAQ' button in the top right is also highlighted with a blue speech bubble.

**Parâmetros do server**

**Parâmetros do Usuário**

# Criação de Malwares

**Agobot Config GUI**

vuln\_channel - String  
 inst\_polymorph - Boolean  
 scaninfo\_chan - String  
 sniffer\_channel - String  
 sniffer\_enabled - Boolean  
 spam\_aol\_enabled - Boolean  
 spam\_aol\_channel - String  
 scaninfo\_level - Integer  
 cdkey\_windows - Boolean  
 identd\_enabled - Boolean  
 redir\_maxthreads - Integer  
 ddos\_maxthreads - Integer

Root Server
  Use SSL

ed.[redacted].com:6667 - #phatrab# - pB-  
 [redacted].ma.cx:6667 - #phatrab# - pB-

gh3tt0 - User32 - User32

I RTFA and I'm really impressed with the features on this trojan.

Server:    
 Server Password:   
 Main Channel:   
 Channel Password:   
 Nick Prefix:

Username:   
 Password:   
 Hostmask:   
 Identmask:   
 Polymorph Section Name:  Key Length:

# 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)
  - Pirataria (warez, videos, livros...)
  - Lucro (DDoS for hire!)
    - “Quer pagar quanto!?”™

```
mIRC - [Status: [-_-]22348 [+ix] on [redacted] (irc [redacted])]
File View Favorites Tools Commands Window Help
# [redacted] [-_-]223... # [redacted] # 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]!~x324512@[redacted]-081-010.[redacted].net.br
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 iowghraAsORTUSxNCWqBzvdHtGp lvhopsmntikrRcaq0ALQbSeKVFHGCuzNT
MAP KNOCK SAFELIST HCN MAXCHANNELS=10 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307
MAXTARGETS=20 AWAYLEN=307 are supported by this server
WALLCHOPS WATCH=128 SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaoHV)~&@%+ CHANMODES=be,kfL,l,psmti
rRcoAQKUGCuzNSMT NETWORK=[redacted] CASEMAPPING=ascii EXTBAN=~ ,cqr ELIST=MNUCT 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
MOTD File is missing
```

Informações do Botnet

# Botnets

The screenshot shows the mIRC IRC client interface. At the top, there is a menu bar (File, View, Favorites, Tools, Commands, Window, Help) and a toolbar with various icons. Below the toolbar, there is a channel list window titled "3/3 Channels on irc. [redacted] Sat Oct 23 08:13:29 2004". The channel list contains the following entries:

513	[+smntCuN]	.advscan lsass_445 150 4 0 -b -r -s
2	[+nt1]	
1	[+nt0]	

A blue arrow points to the second channel, "[+nt1]". Below the channel list, a channel window is open for "# [redacted]# [1] [+CmnNstu]: .advscan lsass\_445 150 4 0 -b -r -s". The window displays the following text:

```
* Now talking in # [redacted]#
* 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
```

On the right side of the channel window, there is a vertical scroll bar and a text area containing the number "cc324512".

# RxBot – Base de 17 exploits!

rxbot (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment Protect SFX

rxbot.archive, unpacked size 852.100 bytes

Name	Size	Packed	Type	Modified	CRC32
Pasta					
advscan.cpp	14.816	4.446	File cpp	9/5/2004 00:15	F7EA5473
advscan.h	1.689	500	File h	13/4/2004 01:21	E6DF01D0
aliaslog.cpp	4.418	1.487	File cpp	11/4/2004 20:39	7912074A
aliaslog.h	867	430	File h	12/4/2004 03:36	9D3DC1F2
authors.txt	346	248	Documento de texto	1/5/2004 14:30	4E1B5BF8
autostart.cpp	953	532	File cpp	9/4/2004 18:20	F547B68E
autostart.h	192	175	File h	9/4/2004 18:20	666E66C4
avirus.cpp	4.454	1.272	File cpp	13/4/2004 00:20	9A239AE7
avirus.h	161	129	File h	13/4/2004 00:20	2CC02EC7
beagle.cpp	1.819	873	File cpp	13/4/2004 00:39	E5BCE275
beagle.h	54	54	File h	13/4/2004 00:39	D07C0AB1
capture.cpp	7.437	1.809	File cpp	9/4/2004 18:20	D9354FD9
capture.h	1.888	502	File h	9/4/2004 18:20	9B1DC1BA
cdkeys.cpp	6.846	1.832	File cpp	11/4/2004 02:06	CA246694
cdkeys.h	221	165	File h	9/4/2004 18:20	0B3EBF18
configs.h	2.820	1.213	File h	16/5/2004 13:39	F60956FD
crc32.cpp	4.598	2.013	File cpp	12/4/2004 03:16	42E419BE
crc32.h	83	73	File h	9/4/2004 18:20	44DD945D
crypt.cpp	18.226	5.349	File cpp	14/4/2004 10:39	B1571E5D
crypt.h	781	320	File h	9/4/2004 18:20	B9B7F19A

Selected 14.816 bytes in 1 file      Total 852.100 bytes in 138 files

# Botnets

mIRC

File View Favorites Tools Commands Window Help

Status: [x]03887786 [+iwx] on [redacted].Com (irc.[redacted].Com)

# [redacted] # [705] [+ntu]: .advscan upnp 150 4 0 -b -r -s

<[x]41181938> [SCAN]: Random Port Scan started on [redacted].x.x:1433 with a delay of 5 seconds for 0 minutes using 150 threads.

<[x]09206286> [SCAN]: Random Port Scan started on [redacted]101.x.x:1433 with a delay of 5 seconds for 0 minutes using 150 threads.

<[x]07944192> [SCAN]: Random Port Scan started on [redacted].x.x:1433 with a delay of 5 seconds for 0 minutes using 150 threads.

<[x]34765064> [SCAN]: Random Port Scan started on [redacted].20.x.x:1433 with a delay of 5 seconds for 0 minutes using 150 threads.

<[x]16308211> [SCAN]: Random Port Scan

@ss  
@xDSSL  
[M][x]10857440  
[M][x]20034367  
[M][x]33074166  
[M][x]64124087  
[x]95610192  
00335734  
00336009  
[x]00652031  
[x]01067380  
[x]01117134  
[x]01423333  
[x]01433675  
[x]01634401

Atividades

Bots

# Botnets

mIRC

File View Favorites Tools Commands Window Help

SomeNet.Com ... # [redacted] # Channels

Status: [x]03887786 [+iwx] on [redacted].Com (irc.[redacted].Com)

# [redacted] [808] [+nt]: .advscan lsass\_445 150 3 0 -b -r -s

to IP: [redacted].109.249 (C:\WINNT\system32\lsass34.exe).

<[x]99052293> [lsass\_445]: Exploiting IP: [redacted].251.236.

<[x]66254409> [lsass\_445]: Exploiting IP: [redacted].85.168.

\* [x]14318525 has quit IRC (Ping timeout)

<[x]97746432> [lsass\_445]: Exploiting IP: [redacted].54.224.

\* [x]80906968 has quit IRC (Ping timeout)

\* [x]52077712 has quit IRC (Connection reset by peer)

\* [x]03813472 has joined #mmansons#

\* [x]83724767 has quit IRC (Ping timeout)

\* [x]24975548 has quit IRC (Ping timeout)

[x]46195141

[x]46262596

[x]46286302

[x]46475276

[x]46673450

[x]46738017

[x]46793512

[x]46946459

[x]47075034

[x]47245680

[x]47281136

[x]47521244

[x]47524817

[x]47733832

[x]47743335

[09:52] <randomnick> .scanstop -s

[09:52] <[x]88804582> [FTP]: File transfer complete to IP: xx.xxx.12.92  
(C:\WINDOWS\System32\lsass34.exe).

[09:53] <randomnick> .advscan lsass\_445 100 3 0 -r -c

[09:53] <[x]10568877> [SCAN]: Random Port Scan started on xx.152.x.x:445 with a delay of 5 seconds for  
0 minutes using 100 threads.

[09:53] <[x]02887235> [SCAN]: Random Port Scan started on xxx.168.x.x:445 with a delay of 5 seconds for  
0 minutes using 100 threads.

[09:53] <[x]38093578> [SCAN]: Random Port Scan started on xx.134.x.x:445 with a delay of 5 seconds for  
0 minutes using 100 threads.

[09:53] <[x]16490013> [SCAN]: Random Port Scan started on xx.168.x.x:445 with a delay of 5 seconds for  
0 minutes using 100 threads.

[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

---

- Estadísticas:

[10:43] <[x]51305501> [SCAN]: Exploit Statistics:  
WebDav: 0, NetBios:0, NTPass: 0, Dcom135: 0,  
Dcom1025: 0, Dcom2: 0, IIS5SSL: 0, MSSQL: 0,  
Beagle1: 0, Beagle2: 0, MyDoom: 0, **Isass\_445: 37**,  
Optix: 0, UPNP: 0, NetDevil: 0, DameWare: 0, Kuang2:  
0, Sub7: 0, **Total: 37 in 0d 17h 29m.**

- Mas como detectar ?

- Conhecendo seu inimigo!

- Entender o funcionamento dos Bots
    - Analises de Bots
      - <http://www.lurhq.com/phatbot.html>
    - Handlers Diaries no ISC ( <http://isc.sans.org> )

- 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 ??
    - Atenção as portas fora 6666:7000
    - Felizmente: Poucos servers com SSL!

- Flows

- Artigos no SecurityFocus

# Botnets

---

- Darknets!

- Monte uma darknet e observe o tráfego para aquele espaço de Ips!
- Um espaço de endereços de uma darknet não deve ser utilizado por ninguém!
- Scanning nessas darknets podem revelar muitas informações
- Atenção a scanning simultâneos:

- Porta 135

- Porta 445

- Porta 80

<http://www.cymru.com/Darknet/>

- Porta 3127

- Porta 2745

- Porta 6129

# Combates a Bots e Botnets

---

- Após a suspeita, como detectar uma Botnet verdadeira?
- 1) Botnet Exclusiva
- 2) Botnet Compartilhada

# 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 a Bots e Botnets

- 1) Botnet Exclusiva
  - Utilizada com o único propósito de ser o ponto focal dos Bots
  - Padrão:
    - Muitos Usuários Invisíveis
    - Unreal é um server muito utilizado

```

Welcome to the [redacted] IRC Network [redacted]!~x324512@[redacted]-081-010.[redacted].net
.br
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 iowghraAsORTUSxNCWqBzvdHtGp lvhopsmtikrRcaqOALQbSeKUFMGCuzNT
MAP KNOCK SAFELIST HCN MAXCHANNELS=10 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307
MAXTARGETS=20 AWAYLEN=307 are supported by this server
MALLCHOPS WATCH=128 SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qao)~&@%+ CHANMODES=be,kFL,l,psmti
RcOAQKUGCuzNSMT NETWORK=[redacted] CASEMAPPING=ascii EXTBAN=~,,cqnr ELIST=MNUCT are supported by
this server
-
There are 1 users and 3815 invisible on 1 servers
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
  
```

# Combates a Bots e Botnets

---

- Botnet Compartilhada
  - São botnets que operam em servidores legítimos de IRC
  - Servidores como Undernet, Effnet não vão ser fechados por causa de um ou outro canal com bots
    - Mas os Operadores dos servidores estão colaborando nessa detecção!
  - Nesse caso as informações de Usuários são inúteis
    - Opção: Detecção do Canal utilizado

# 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://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>

## O futuro...

---

- Ed Skoudis, Handler do ISC, prevê um combo-malware:
  - Kernel mode rootkit...  - (Hacker Defender?)
  - Código polimorfico...  - (Morphine?)
  - Dentro de um bot...  (ago|phat|SD|Rbot ?)
  - Distribuído por um worm...  ...?
  - Altere a bios para assegurar a reinstalação...

Tudo em um pacote!

# 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!

# Conclusões

---

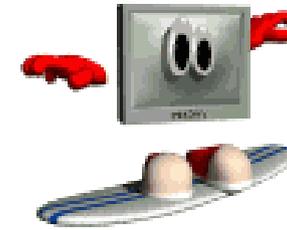
- O desenvolvimento cada vez mais rápido por parte dos fabricantes de malwares pede uma ação também rápida, fabricantes de AV no desenvolvimento de vacinas e de usuários finais e administradores, no aplicação dos patches!
- A comunidade precisa se organizar estabelecendo linhas de comunicação eficientes de modo a responder também de forma rápida a essas ameaças!
- Assegurar que os sistemas contem com uma configuração segura (Hardened Systems) possibilita um importante ponto de defesa na luta contra os malwares.
- Lembre-se: Worms não são indicações de Patch-time!

# 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> , [handlers@sans.org](mailto:handlers@sans.org))
- Aprenda a fazer um hardening do seu sistema  
(<http://www.sans.org>)



[pbueno@isc.sans.org](mailto:pbueno@isc.sans.org) / [bueno@ieee.org](mailto:bueno@ieee.org)

---

# Conclusões

- E...estamos no caminho certo!

The screenshot shows a Mozilla Firefox browser window with the following elements:

- Address Bar:** <http://www.pcworld.com/news/article/0,aid,116077,00.asp>
- Navigation:** Back, Forward, Reload, Home, Stop, Search (Google), and a search box containing "tydooom source code".
- Browser Tabs:** PCWorld.com - German Police Snag P..., SANS - Internet Storm Center - Cooperativ..., Symantec Search.
- Advertisements:** A large banner for XEROX with the text "ENDURANCE 2400 dpi at 26 ppm. Color printing that won't quit." and the XEROX logo.
- Page Header:** "TECHNOLOGY ADVICE YOU CAN TRUST" on the left and "SEPTEMBER 12, 2004" on the right.
- Navigation Menu:** HOME | NEWS | REVIEWS | HOW-TO | DIGITAL WORLD | DOWNLOADS | TOOLS | PRODUCT FINDER | MAGAZINE.
- Search and Browse:** A search box with a "SEARCH" button, a "USE FIND.PCWORLD.COM" button, and a "BROWSE BY TOPIC" button.
- Product Guides:** Cameras, Notebooks, Desktops, Printers, Monitors, Home Networks, PDAs.
- Related Articles:**
  - [Teenager Charged With Creating Sasser](#)
  - [Al Qaeda's Tech Traps](#)
  - [Dozens Convicted of Cybercrimes](#)
  - [Online Extortion Ring Broken Up](#)
  - [Antipiracy Efforts Seek Funding](#)
- Main Article:**
  - Topic Breadcrumbs:** [Topics](#) > [Privacy & Security](#) > [Cybercrime](#) >
  - Headline:** **German Police Snag Phatbot Author**
  - Sub-headline:** Capture coordinated, but not linked, with Sasser arrest, police say.
  - Author:** Paul Roberts, IDG News Service
  - Date:** Monday, May 10, 2004
  - Text:** A 21-year-old German man was arrested and has admitted to creating the ubiquitous and dangerous Trojan horse programs Agobot and Phatbot, but he is not connected to the German author of the Sasser Internet worm, a police spokesman said.
  - Text:** German police arrested the man on Friday in the southern German town of Waldshut and charged
- Footer:** "Transferring data from www.pcworld.com..." and a status bar with green progress indicators.

# Referencias

---

- **SANS Internet Storm Center – [isc.sans.org](http://isc.sans.org)**
- **Botnet and DDoS mitigation for ISPs - CPN Summit 2004 - <ftp://ftp-eng.cisco.com/cons/isp/security/>**
- **NSP-SECurity List Homepage - <https://puck.nether.net/mailman/listinfo/nsp-security>**
- **DarkNet Project – <http://www.cymru.com.br/Darknet>**



**[FIM!]**

**[pbueno@isc.sans.org](mailto:pbueno@isc.sans.org) / [pbueno@gmail.com](mailto:pbueno@gmail.com)**

**61 8401-1977**