Probe

Sistema Automatizado de Tratamento de Incidentes envolvendo *Probes* e *Scans*

Luiz Eduardo R. Cordeiro Klaus Steding-Jessen

Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil — CERT.br
http://www.cert.br/

Comitê Gestor da Internet no Brasil — CGI.br
http://www.cgi.br

Roteiro

Motivação

Trabalhos Relacionados

Protótipo do Sistema

Estatísticas dos Testes com o Protótipo

Trabalhos Futuros

Motivação

Trabalhos Relacionados

Protótipo do Sistema

Estatísticas dos Testes com o Protótipo

Trabalhos Futuros

Motivação

Análise e notificação de *logs* de *Probes* e *Scans*:

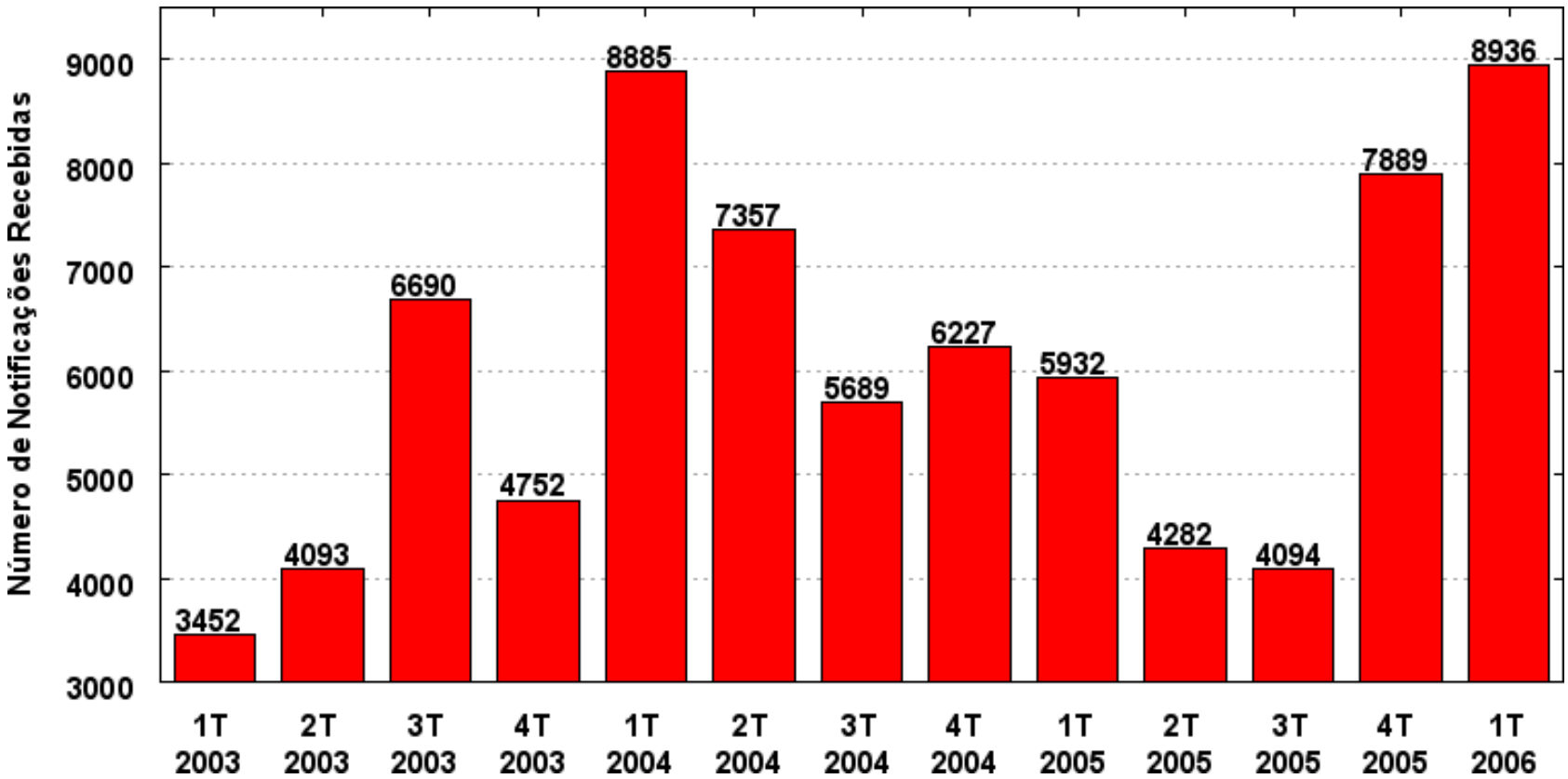
- podem fornecer um panorama geral do que está ocorrendo na *Internet*;
- fornecem fortes indícios de atividades vindas de máquinas possivelmente comprometidas;
- auxiliam na análise de tendências sobre incidentes de *scan*.

Motivação (cont.)

- Auxiliar administradores de redes que, raramente dispõe de tempo para:
  - analisar os *logs* dos diversos *firewalls* e *IDS*;
  - selecionar *logs* mais importantes;
  - pesquisar contatos de redes; e
  - enviar e acompanhar as notificações.

Notificações Recebidas pelo **CERT.br**

Quantidade de notificações de Incidentes relacionados a *Scans* recebidas pelo **CERT.br**:



Motivação

Trabalhos Relacionados

- AusCERT — Probe
- SANS Internet Storm Center
- CERT/CC — AirCERT

Protótipo do Sistema

Estatísticas dos Testes com o Protótipo

Trabalhos Futuros

AusCERT — Probe

"Automated incident report processing and cross-correlation of probe and scan information"
Mark McPherson (FIRST, 2001) [1]

- Recepção de *e-mails* contendo identificadores especiais.
- Tratamento semi-inteligente dos *e-mails* normais.
- Tratamento diferente entre membros e não-membros do **AusCERT**.
- Banco de dados para correlação das informações.

[1] http://www.first.org/events/progconf/2001/D4-05.pdf.gz

SANS Internet Storm Center

SANS Internet Storm Center (ISC) [2]

- Criado em 2001 após o aparecimento do *Li0n Worm*.
- Atualmente é um sistema gratuito de análises e avisos destinado a usuários da Internet.
- Todas as etapas deste serviço são totalmente realizadas por voluntários.
- *Scripts* para *logs* de vários *firewalls*, *IDS* e sistemas operacionais.
- Dados coletados alimentam o banco de dados *DShield*.
- Existe a opção dos incidentes serem notificados (*FightBack*).

[2] http://isc.sans.org/

CERT/CC — AirCERT

AirCERT *— Automated Incident Report* [3]

- Visa a troca de informação sobre eventos de segurança.
- Objetivo é prover a capacidade de discernir tendências e padrões de atividades.
- *Analysis Console for Intrusion Databases*
  - Interface de pesquisa.
  - Visualizador de pacotes.
  - Gerenciador de alertas.
  - Estatísticas.

[3] http://www.cert.org/kb/aircert/

Motivação

Trabalhos Relacionados

Protótipo do Sistema
- Decisões Importantes
- Componentes Principais do Sistema

Estatísticas dos Testes com o Protótipo

Trabalhos Futuros

Decisões Importantes

- Necessidade de um sistema simples do ponto de vista do administrador de sistemas.
- Concentração do esforço computacional no **CERT.br**.
- Flexibilidade quanto aos tipos diferentes de *logs*.
- Informações de tempo e *timezone* são absolutamente relevantes.
  - Máquinas devem estar sincronizadas (*NTP*).
  - Horário de verão.
- Alguns tipos de *logs* não fornecem dados precisos sobre ano e *timezone*.
  - `tcpdump` possui opção (`-tt`) de fornecer tempos em *Epoch*;
  - Uso do `syslog-ng` com opção de formatação de datas ISO8601: `YYYY-MM-DD hh:mm:ss +TTTT`.

Configuração do `syslog-ng`

- Exemplo de configuração do `syslog-ng` para um arquivo de *log* localizado em `/var/log/firewall.log`:

```
destination security {
 file("/var/log/firewall.log"
  template("$ISODATE $HOST $MSG\n")
  template_escape(no)
 );
};
```

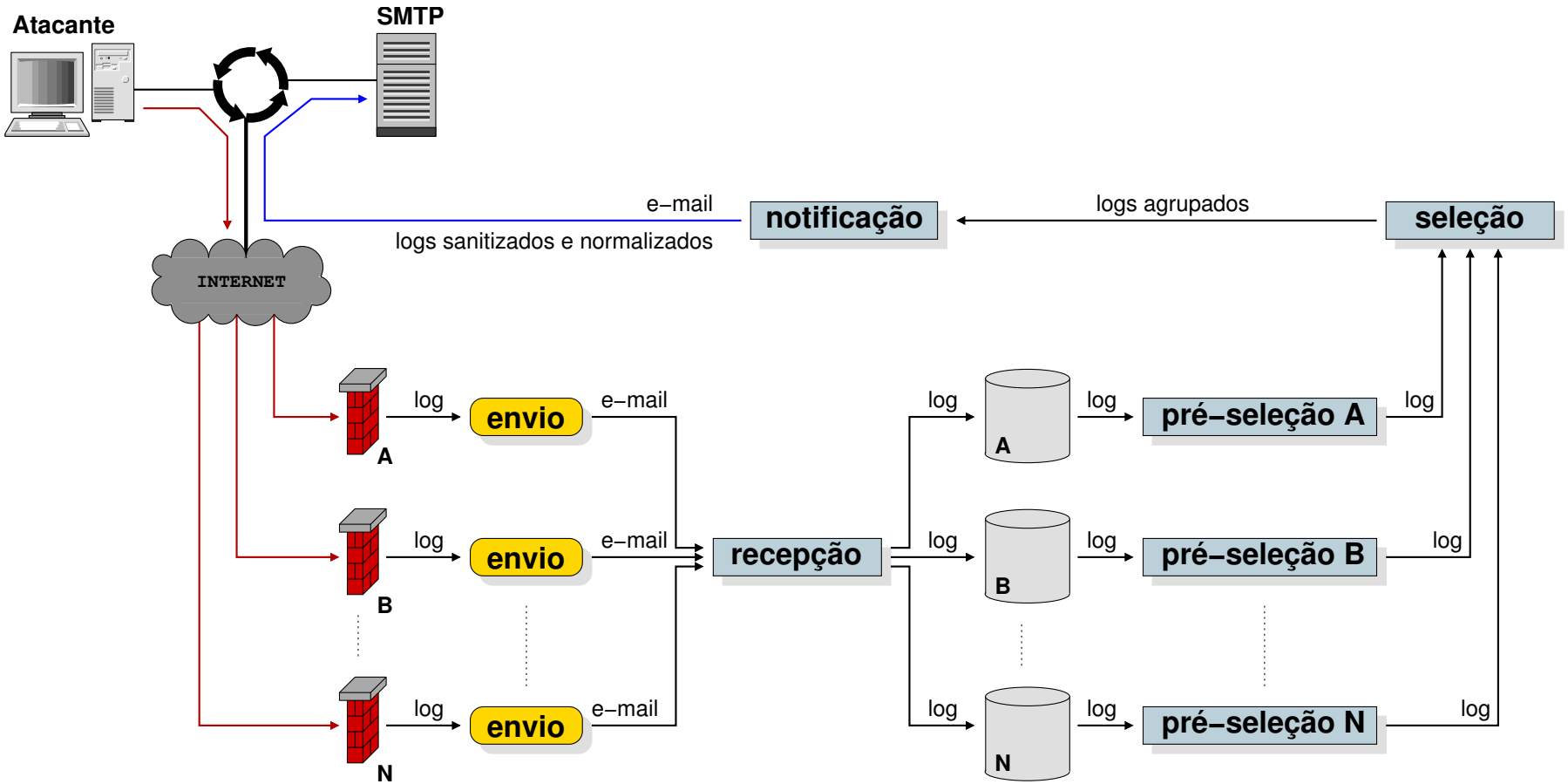
- Exemplo de *log* neste formato (`iptables`):

```
2006-06-02T17:34:56+03:00 [HOST] kernel: ...
 SRC=[IP] DST=[IP] ...
 PROTO=TCP SPT=35745 DPT=22 ...
 SYN URGP=0
```

Componentes Principais do Sistema

- Envio dos *Logs*.
- Recepção dos *Logs*.
- Seleção dos *Logs*.
- Sistema de Notificação.

Probe — Diagrama



Envio dos *Logs*

- Envio dos *logs* com comandos tão simples quanto:
  - `zcat firewall.log.gz | probe_send_logs.pl`
  - `tcpdump -tt -r /var/log/pf.log | ...`
- Envia os *e-mails* em *chunks* de tamanhos definidos pelo administrador.
- Utiliza `gpg` para codificar e comprimir os *logs*.
- Utiliza `mail` ou `mutt` para envio dos *logs*.

Exemplo de Configuração

```
Email-To:          no-email@cert.br
Email-Cc:          email1@exemplo.com
Email-Bcc:         email2@exemplo.com
GPG-Cmd:           /usr/local/bin/gpg
GPG-Cipher:        blowfish
GPG-Compress:      default
GPG-Passphrase:    [chave-simétrica]
Tmpdir:            /tmp
Max-Log-Size:      20 M
Max-Chunk-Size:    1 M
```

Recepção dos *Logs*

- Verifica a origem dos *logs*:
  - *From envelope* do *e-mail*;
  - *MTA Server* que enviou o *e-mail*; e
  - Chave simétrica.
- Decodifica e descompacta os *logs* enviados.
- Armazena os *logs* para processamento:
  - Padronizados no formato `libpcap`; e
  - Tempos convertidos para *UTC*.
- Formatos suportados até o momento: `tcpdump` e `iptables`.
- Possibilidade de sanitização dos *logs* nesta etapa.

Seleção dos *Logs*

Pré-seleção:

- Utiliza expressões `tcpdump` para selecionar *logs*.
- Regras independentes por instituição.
  - Útil para reduzir a quantidade dos *logs*.
  - Útil para isolar sub-redes ou máquinas específicas.

Seleção:

- Também utiliza expressões `tcpdump` para selecionar *logs*.
- Regras mais genéricas e válidas para todos as instituições.
- Durante a seleção, os *logs* são agrupados por IP de origem.

Sistema de Notificação

- Consulta vários bancos de dados `whois` para obtenção de contatos de redes.
- Permite ajustes de contatos por blocos `CIDR`.
- Normaliza e sanitiza os *logs* antes de enviá-los.
- Gera e envia os *e-mails* para os contatos das redes de origem dos incidentes.
- A partir dos *e-mails* enviados, gera estatísticas de envio.

Motivação

Trabalhos Relacionados

Protótipo do Sistema

Estatísticas dos Testes com o Protótipo

Trabalhos Futuros

Estatísticas de Incidentes Notificados

Mês	Ano	Notificações
Dezembro	2005	122
Janeiro	2006	531
Fevereiro	2006	506
Março	2006	400
Abril	2006	364
Maio	2006	375

O sistema **Probe** encontra-se em avaliação desde 21 de dezembro de 2005.

Probe: *Scans* mais Freqüentes

Primeiro Trimestre de 2006 (1437 notificações)

Posição	Porta	Serviço	Notificações
1	22/tcp	SSH	1267
2	23/tcp	Telnet	79
3	21/tcp	FTP	54
4	111/tcp	SunRPC	31
5	6112/tcp	CDE Ctrl	7
6	1080/tcp	Socks	5
7	3664/tcp	UPS Engine[4]	1
8	515/tcp	Printer	1
9	80/tcp	HTTP	1
10	multi/tcp	Vários	1

[4] Portas de origem e destino idênticas.

Scans mais Freqüentes

Primeiro Trimestre de 2006 (7499 notificações)

Posição	Porta	Serviço	Notificações
1	22/tcp	SSH	3604
2	23/tcp	Telnet	585
3	1080/tcp	Socks	302
4	21/tcp	FTP	270
5	443/tcp	HTTPS	235
6	53/udp	DNS	223
7	25/tcp	SMTP	183
8	143/tcp	IMAP	164
9	8080/tcp	Proxy	145
10	multi/tcp	Vários	133

Probe: Países mais Freqüentes

Primeiro Trimestre de 2006 (1437 notificações)

Posição	País[5]	Notificações
1	China	285
2	Estados Unidos	184
3	Brasil	152
4	Romênia	131
5	Coréia do Sul	121
6	Taiwan	78
7	Índia	45
8	Alemanha	32
9	Japão	31
10	Itália	28

[5] IPs alocados

Países mais Freqüentes

Primeiro Trimestre de 2006 (7499 notificações)

Posição	País[6]	Notificações
1	Brasil	1776
2	Estados Unidos	1203
3	China	1149
4	Coréia do Sul	527
5	Taiwan	522
6	México	177
7	Alemanha	143
8	Índia	139
9	França	138
10	Argentina	117

[6] IPs alocados

Motivação

Trabalhos Relacionados

Protótipo do Sistema

Estatísticas dos Testes com o Protótipo

Trabalhos Futuros

Trabalhos Futuros

- Aumentar o número de formatos de *logs* suportados.
- Implementar um sistema de estatística por instituição colaboradora.
- Melhorar, na medida do possível, o sistema de consulta aos servidores *whois*.

Observação: Não há ainda um prazo definido para que este sistema torne-se público.