2º Fórum Brasileiro de CSIRTs

17 de setembro de 2013

Detecção e Tratamento de Softwares Maliciosos na Rede do Governo do Estado do Paraná

Jose Roberto Andrade Jr
Hermano Pereira
Oeslei Taborda Ribas

CELEPAR INFORMÁTICA do PARANÁ

Agenda

- Atribuições da CELEPAR
- Desafios de um CSIRT Gov.
- Ataques externos de botnet
- IDS (Sistema de detecção de intrusão)
- HoneyPot
- DNS Sinkhole
- Outras Técnicas
- Alertas por e-mail

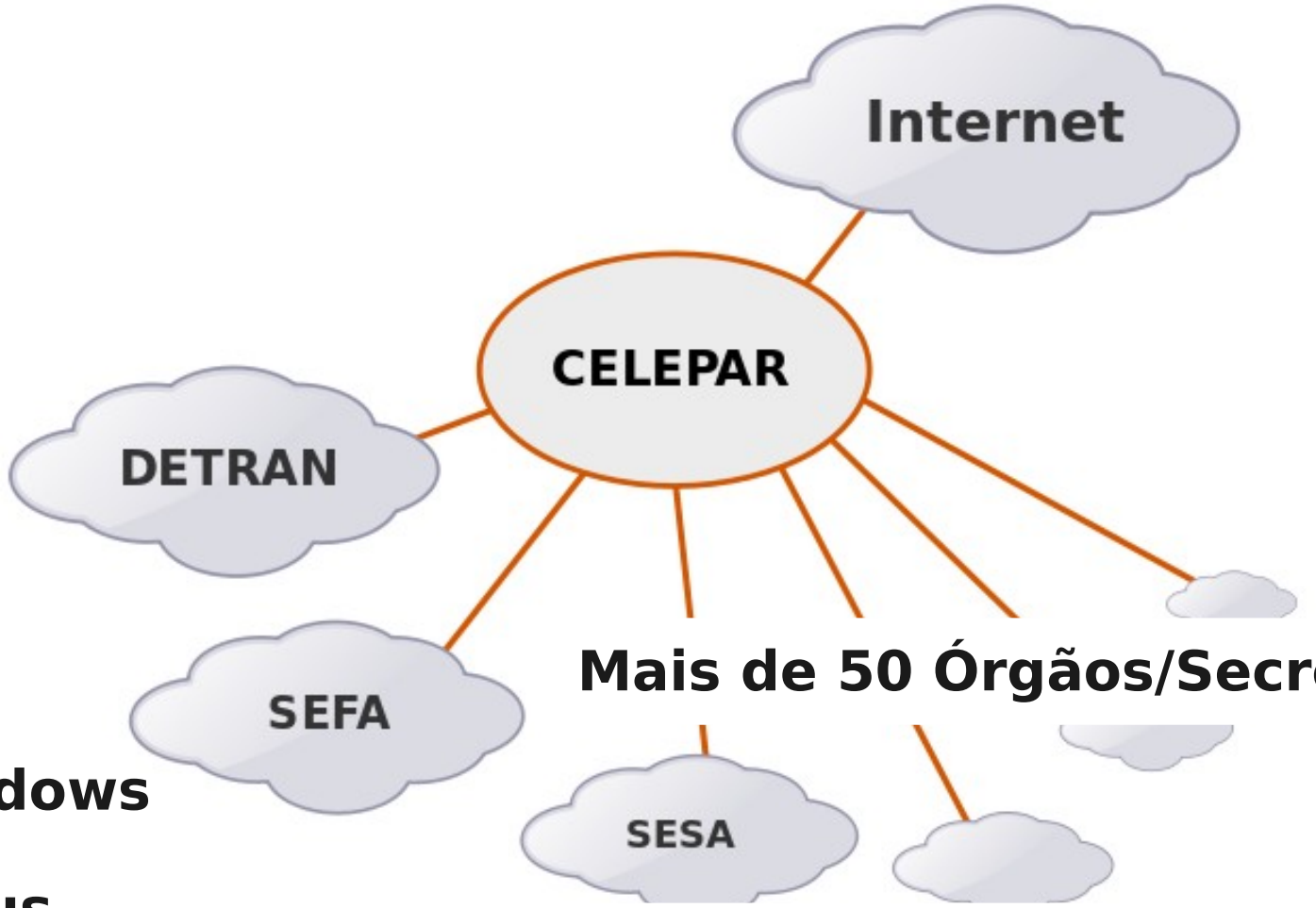
Atribuições da CELEPAR

- CELEPAR
  - Companhia de Informática do Paraná
  - Economia Mista (Governo do Paraná)
  - Responsável pelo domínio .pr.gov.br
  - Responsável pela conectividade das universidades estaduais.
  - Clientes:

    DETRAN, SEFA, SESA, SEED, SESP...

www.celepar.pr.gov.br

Atribuições da CELEPAR



Mais de 50 Órgãos/Secretarias

~45% Windows

Antivírus Corporativo

Mais de 40.000 estações

Desafios de um CSIRT Gov

- Clientes com políticas de segurança da informação diferentes
- Clientes com autonomia em relação as decisões relacionadas a segurança da informação
- Turnover dos profissionais de TI
- Instalação/manutenção de aplicativos de terceiro
- Dificuldades na aquisição de equipamentos e licenças de software

Detecção e Tratamento de Softwares Maliciosos

Ataques externos de botnet

- Ataques de DDoS
- Abuso de formulários
- Ataques a aplicações com CAPTCHA
- Roubo de dados

Tamanduah: Consumo de Banda
TamanduahURL: Requisições a URLs

- Pcap / TCPDump
- TCP / IP
- Espelhamento
  - Firewall, Proxy

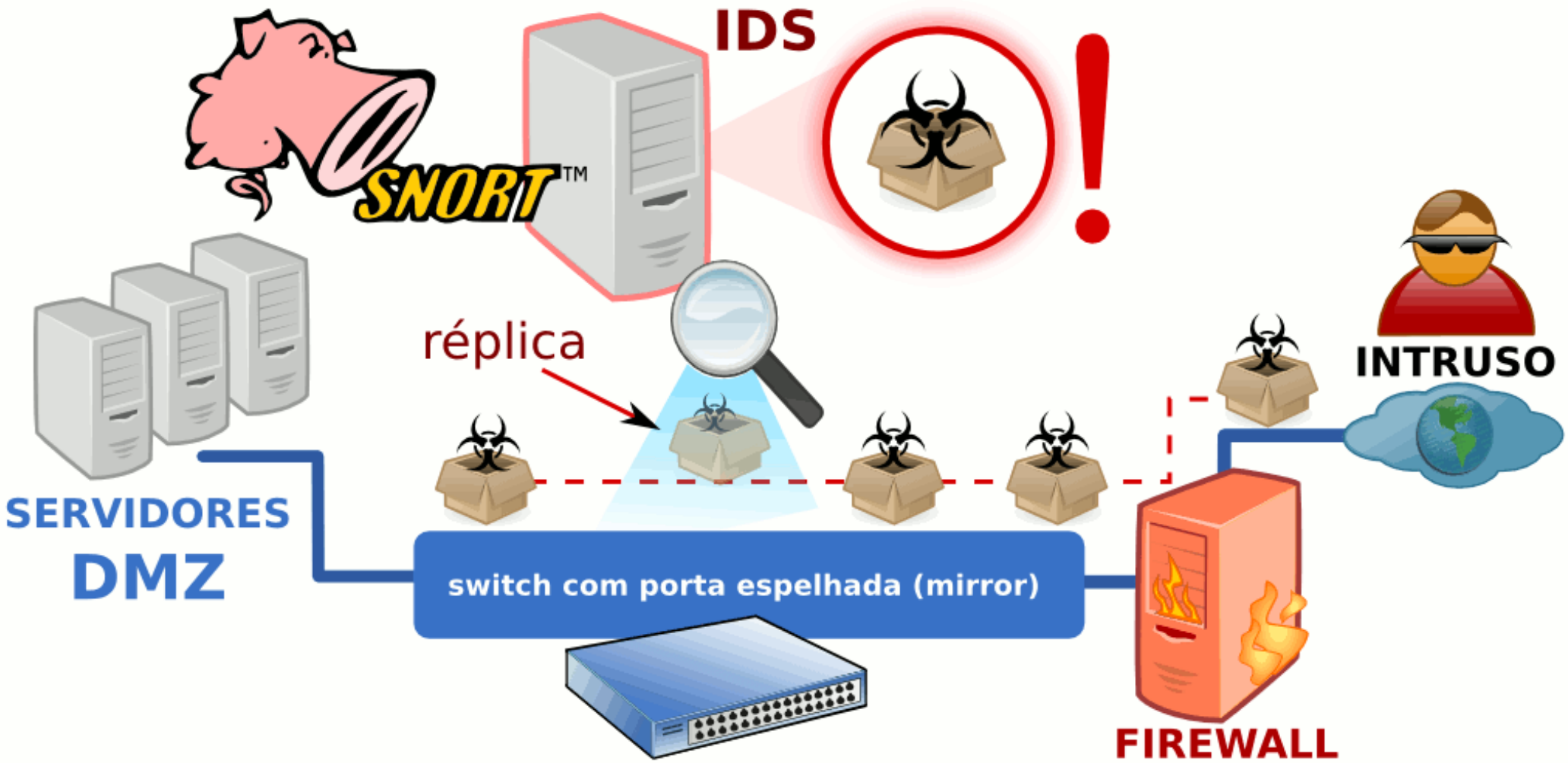
```
perl tamanduah.pl -i eth0 -s 10.0.0.0/8 -d "^10.0.0.0/8,:53" -p udp -q 10

--Tamanduah--2.2-------------------------------------------------------------------------------
     Hosts               Bytes IN                    Bytes OUT                   Bytes Total
-------------------------------------------------------------------------------------------------
1    10.X.X.X            245934          44.54%      82497           41.26%      328431          43.67%
2    10.X.X.X            162296          29.39%      67269           33.64%      229565          30.52%
3    10.X.X.X            130920          23.71%      39905           19.96%      170825          22.71%
4    10.X.X.X            3663            0.66%       818             0.41%       4481            0.60%
5    10.X.X.X            3860            0.70%       518             0.26%       4378            0.58%
6    10.X.X.X            602             0.11%       887             0.44%       1489            0.20%
```

Intrusion Detection System (IDS)

- IDS Snort com assinaturas da Emerging Threats
- Regras por rede
- Assinaturas personalizadas para o nosso ambiente
- Assinaturas feitas sobre demanda para novas ameaças.
- Visão dos alertas por cliente
- Visão dos alertas por malware

Intrusion Detection System (IDS)



CELEPAR INFORMÁTICA do PARANÁ

ARAPONGAH
alertas de segurança

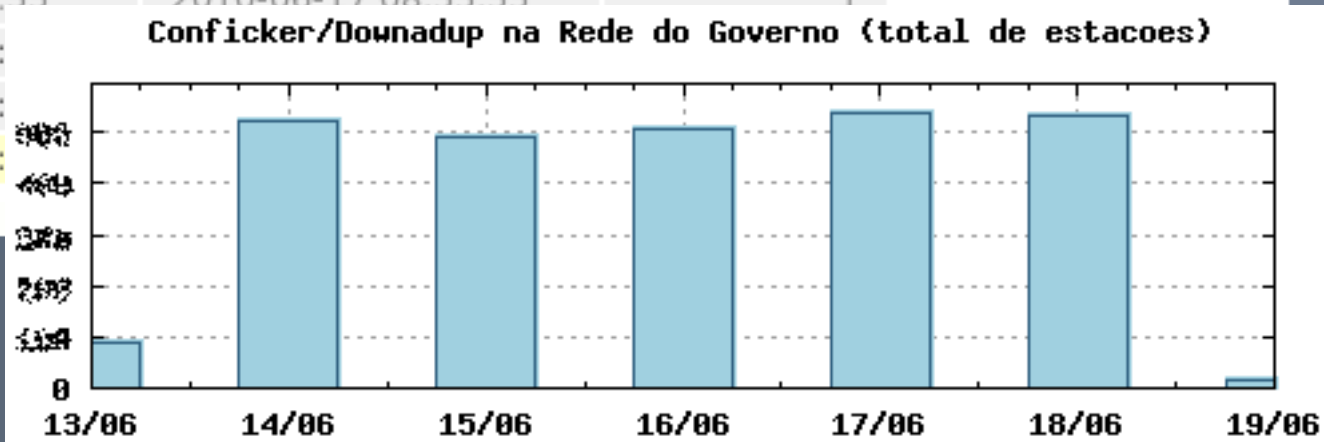
Relatório de estações infectadas pelo vírus Downadup/Conficker

Médio risco

Descrição:	Este tipo de alerta ocorre quando uma estação infectada pelo vírus Conficker e tenta se comunicar com o seu invasor via Internet. A maior parte destas comunicações são barradas pelo firewall. Estações infectadas pelo Conficker são problemáticas pois estão vulneráveis à varredura de variantes e versões recentes do próprio Conficker.
Coleta:	Últimas 48 horas

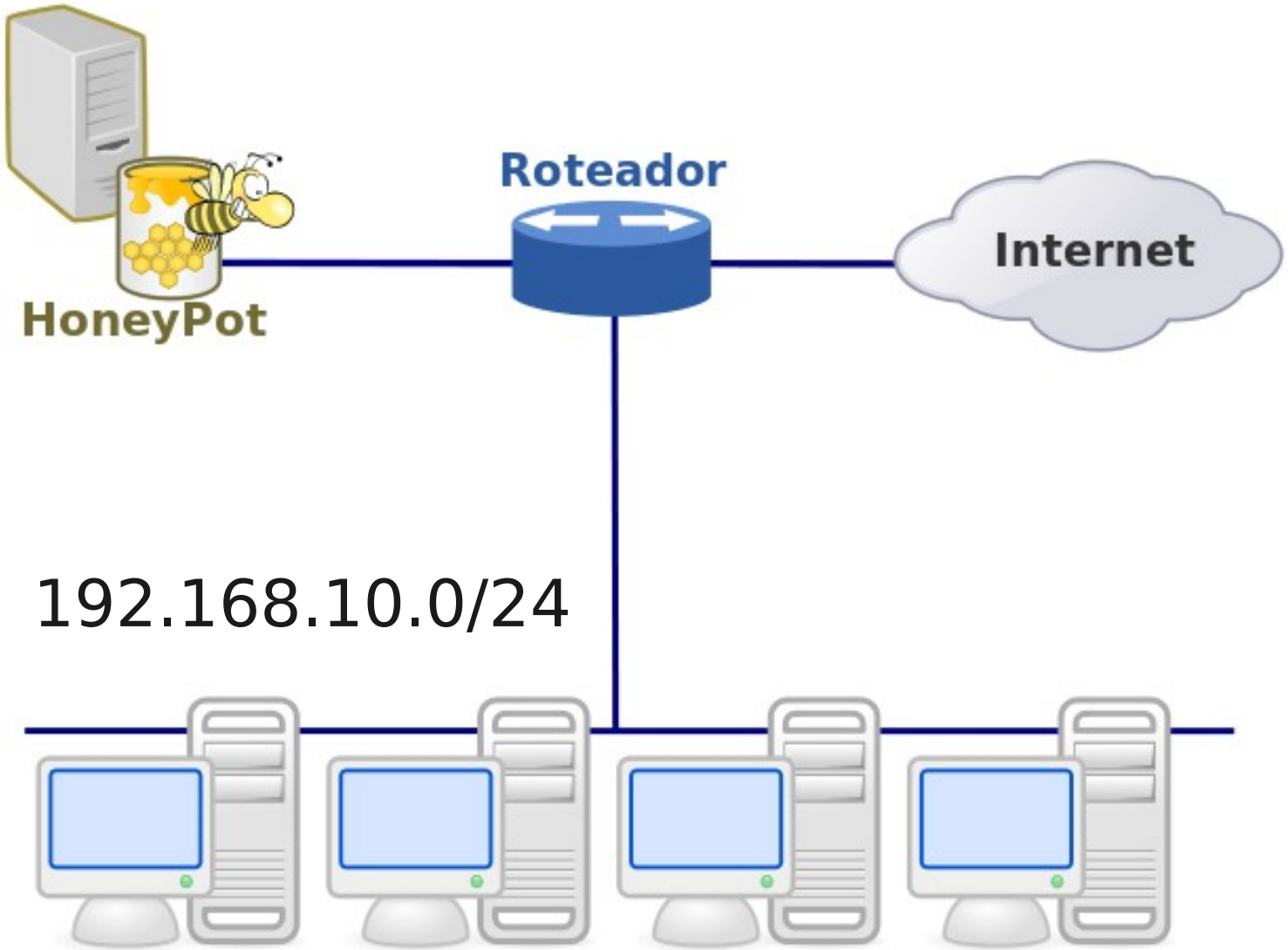
Total de elementos: [illegible] - Total de alertas: [illegible] Última atualização: [illegible]

Estação	Primeiro alerta	Último alerta	Qtde
10.[illegible]	2010-06-17 09:36:59	2010-06-18 10:05:40	2
10.[illegible]	2010-06-17 10:24:14	2010-06-18 10:56:05	3
10.[illegible]	2010-06-17 14:34:43	2010-06-18 14:24:47	2
10.[illegible]	2010-06-17 15:00:37	2010-06-18 20:31:01	3
10.[illegible].155	2010-06-17 07:59:26	2010-06-18 06:32:38	8
10.[illegible].164	**2010-06-17 01:00:50**	**2010-06-18 22:47:03**	**16**
10.[illegible].218	2010-06-17 12:12:41	2010-06-17 12:12:41	1
10.[illegible].226	2010-06-17 08:33:33	2010-06-17 08:33:33	1
10.[illegible]16	2010-06-17 08:50:		
10.[illegible].17	2010-06-17 08:25:		
10.[illegible]27	2010-06-17 08:09:		



CELEPAR INFORMÁTICA do PARANÁ

HoneyPot



HoneyPot

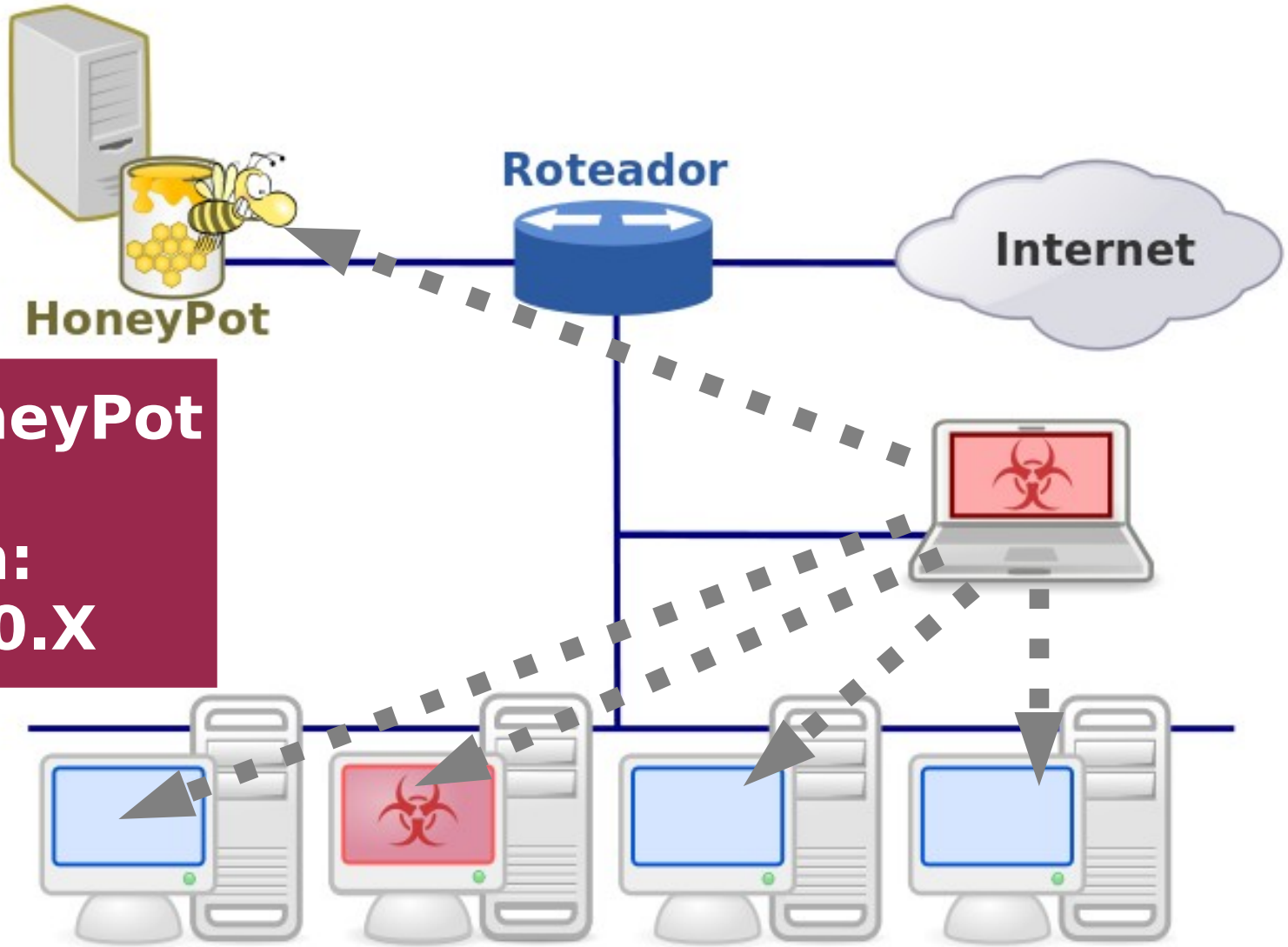
Rotas para o HoneyPot:

RFC 1918
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

RFC 3927
- 169.254.0.0/16

RFC 1112
- 0.0.0.0/8
- 127.0.0.0/8

HoneyPot

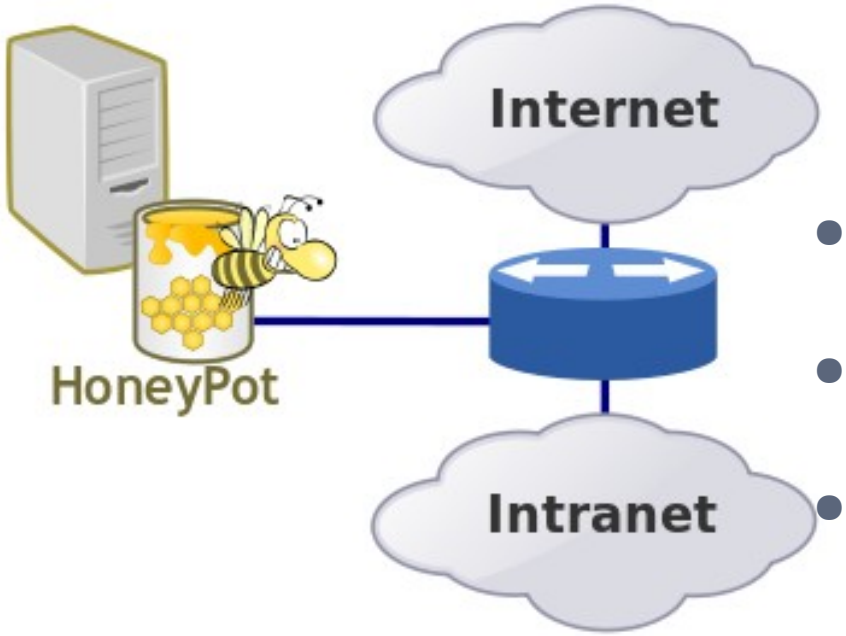


Alerta do HoneyPot

Vírus em:
192.168.10.X

CELEPAR
INFORMÁTICA
do PARANÁ

HoneyPot Corporativo



Hoje:

- 1 Servidor HoneyPot
- Roteamento Switch Core
- Nepenthes, Snort e IPTables

Próximo passo:

- Honeyd/Dionaea
- HoneyPot nos Clientes

HoneyPot nas DMZs

Hoje:

- Servidor HoneyPot em 3 DMZs
- Sem roteamento

Próximo passo:

- Em todas as redes hospedadas

HoneyPot Corporativo

Alguns dados:

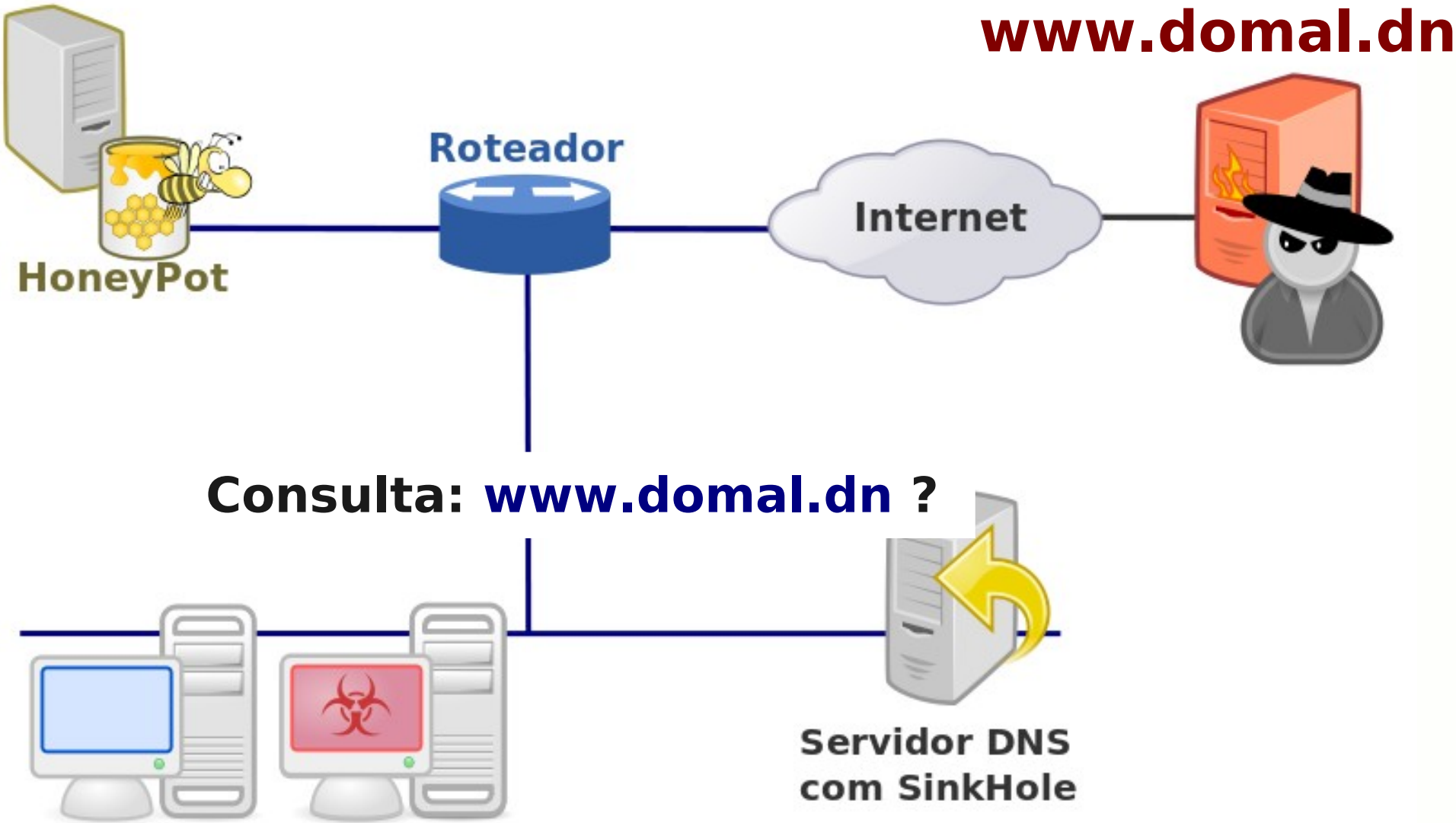
- ~ 35% dos alertas de segurança
- Diversos ataques (Portscan)
- Erros de configuração
- Novos vírus/malwares
- Erros em WebSites

DNS SinkHole

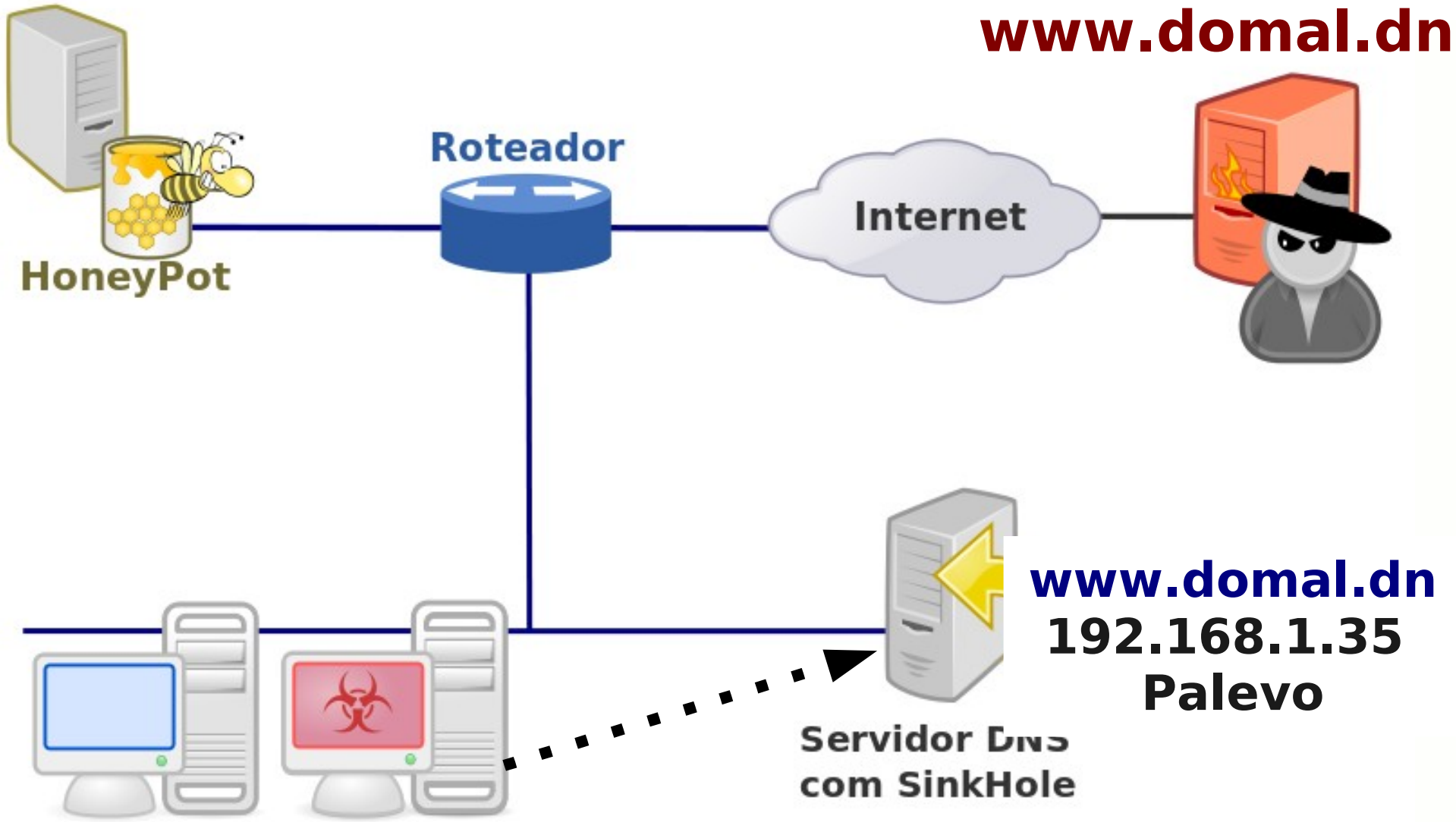
- **DNS SinkHole**

  O DNS SinkHole é um recurso adicionado ao servidor de DNS para resolver domínios que são utilizados para fins maliciosos (vírus). Assim o domínio malicioso poderá ser resolvido para um endereço IP de um HoneyPot.

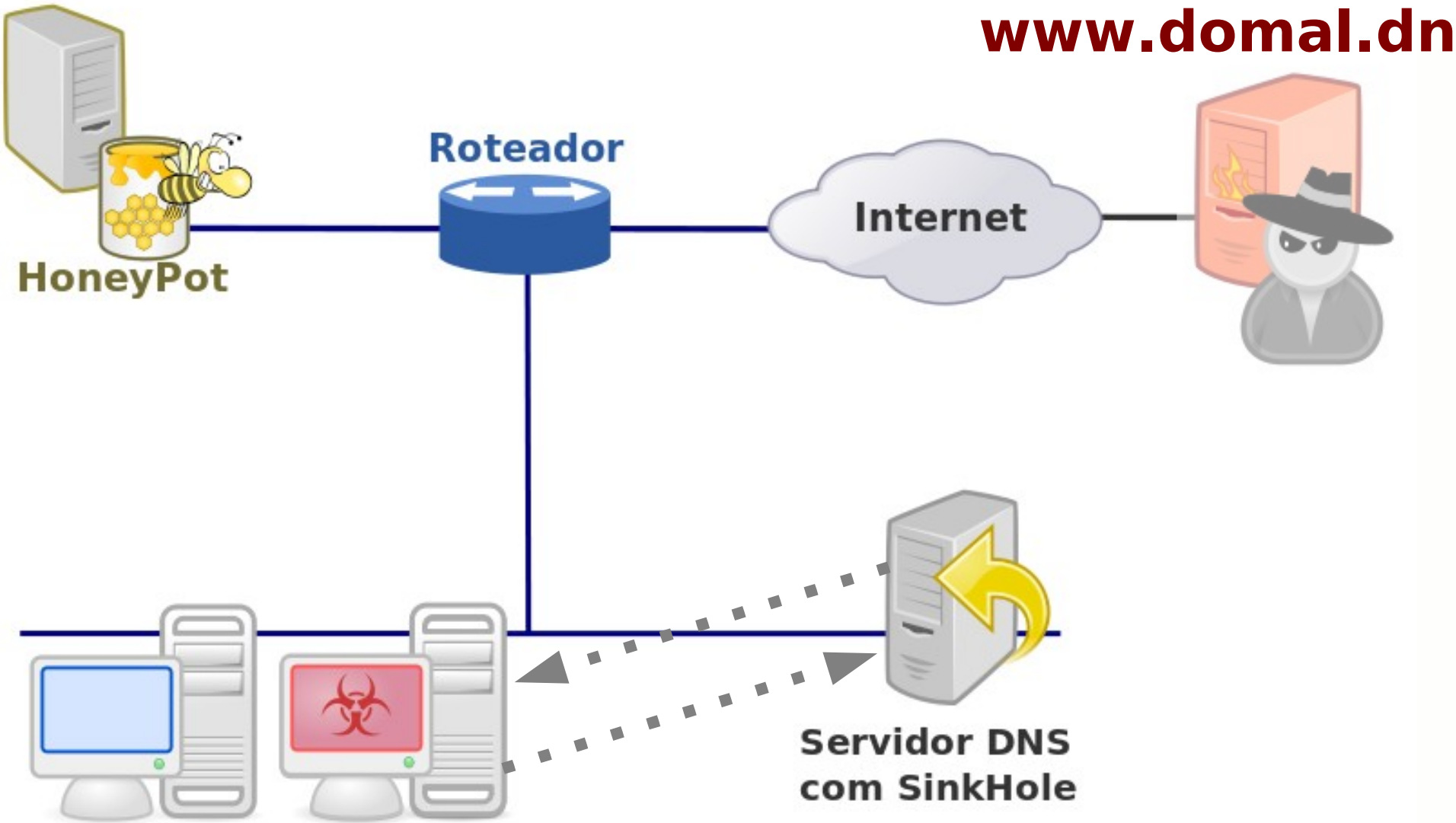
DNS SinkHole



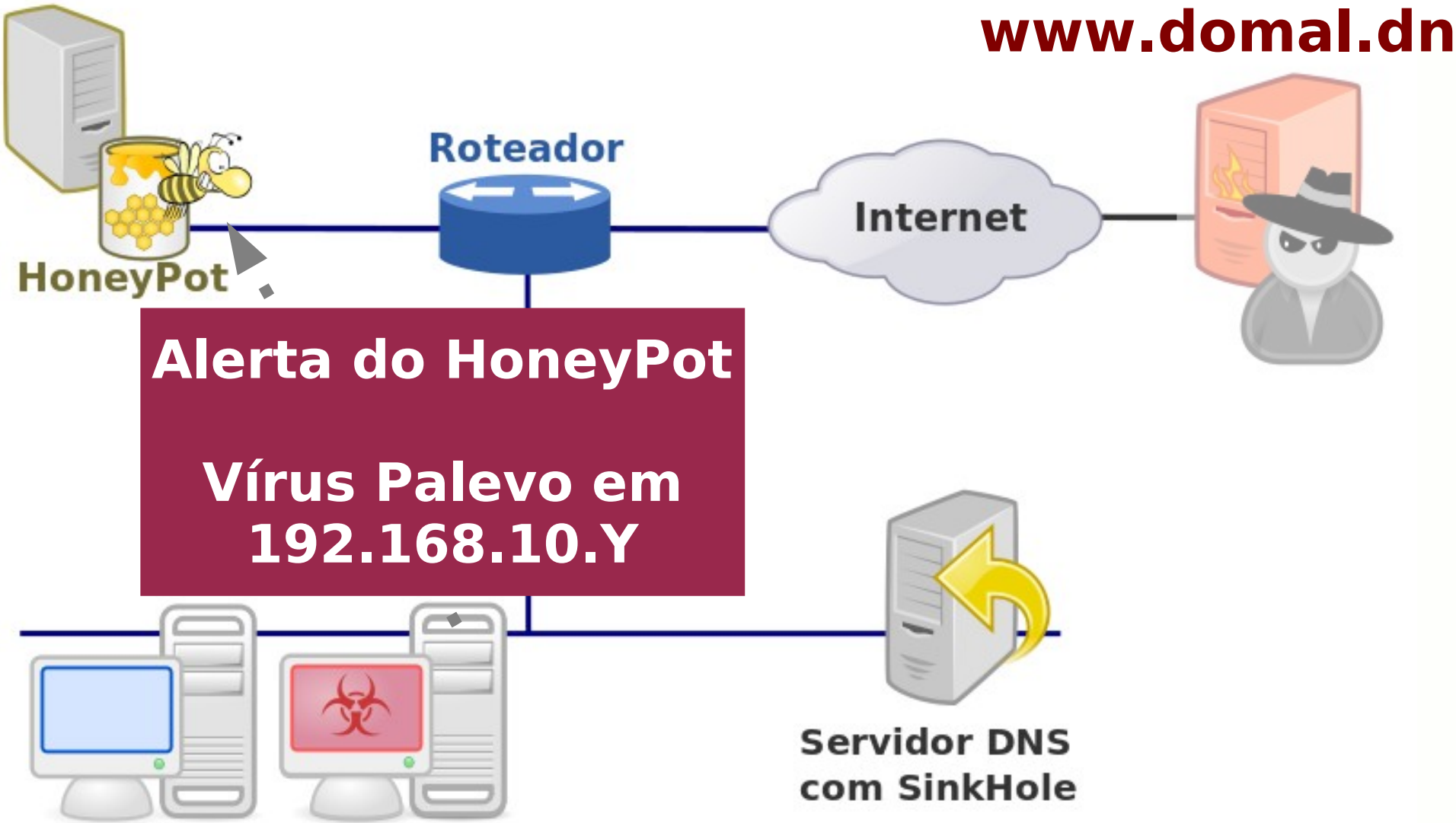
DNS SinkHole



DNS SinkHole



DNS SinkHole



DNS Sinkhole

Hoje:

- 1 Servidor DNS em Teste

  (~2000 hosts)
- SinkHole → ISC Bind
- AMADA e Malware Domain List

Próximo passo:

- DNS Corporativo
- DNS Clientes

Servidor de Logs

- Recebe logs via syslog.
- Log do servidor de antivírus.
- Log dos roteadores.
- Log do antispam.
- Log de alguns servidores.

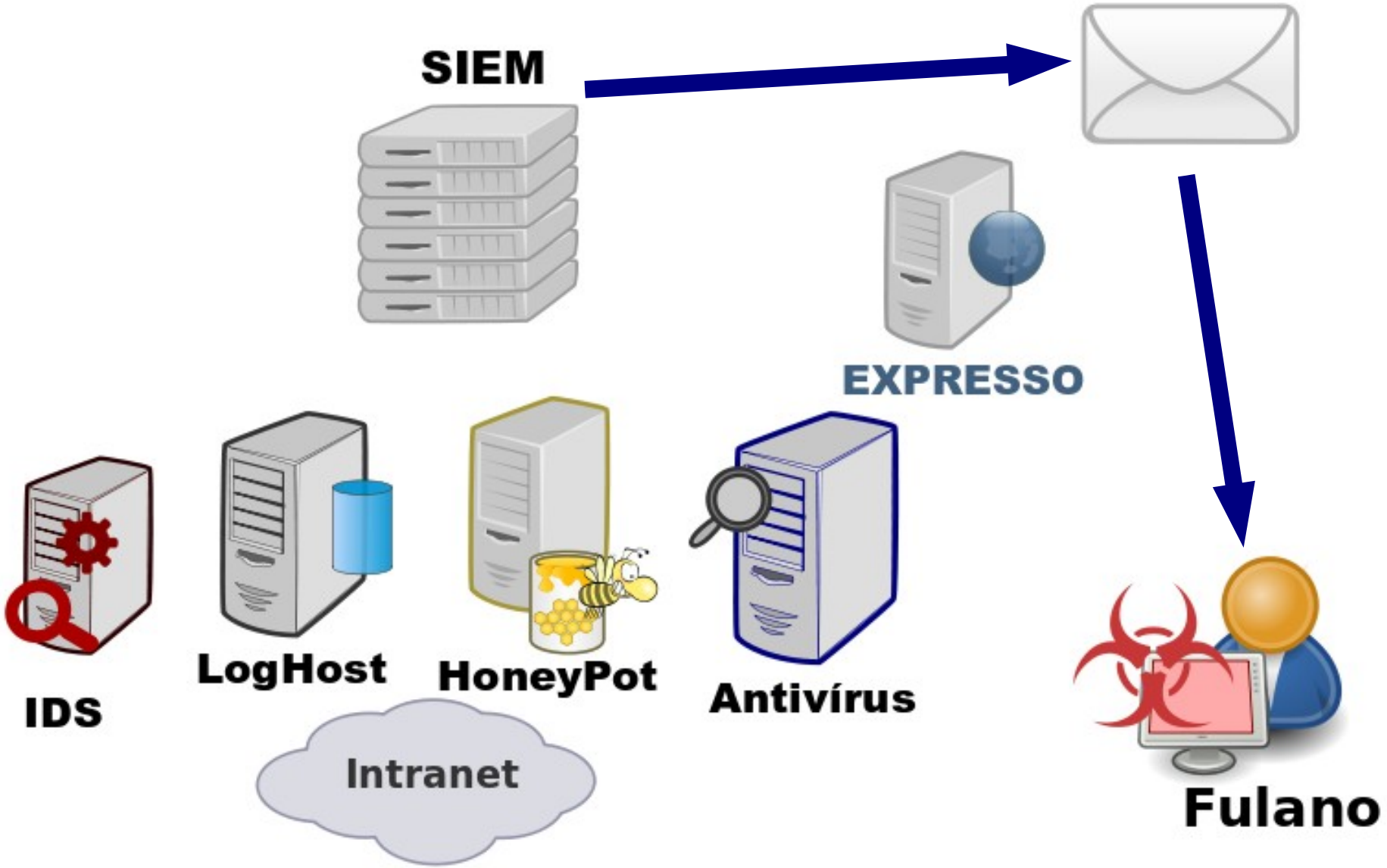
SIEM

- Prelude (http://www.prelude-ids.com/)
- Protocolo IDMEF (RFC 4765)
- Vários módulos (LML, Prewikka, Manager)
- Agentes para diferentes S.O. e aplicações.
- Comunicação criptografada entre os agentes e o manager
- Buffer local para armazenamento

Outras Técnicas

- Análise de logs do Proxy.
- Análise de logs do DNS.
- Análise de logs do Firewall.
- Horário/frequência das requisições.

Alertas por e-mail



Alertas por e-mail

From: Equipe de Segurança

To: Fulano

Subject: [Mensagem Automática]

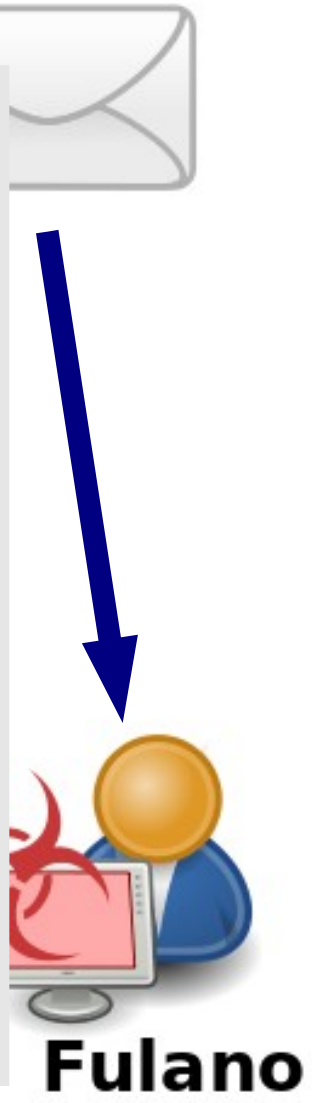
Caro(a) Fulano,

Identificamos que sua estação está com vírus!

Alertas: XYZ

Procedimentos: ABC

Gratos pela sua colaboração!



Conclusão

- As soluções apresentadas permitem Monitorar estações que estão sem o antivírus corporativo
- Detecção de novos vírus e ameaças
- Baixo custo, efetivo
- Escalável e fácil de manter

Referências

- amada.abuse.ch
- [dionaea|nepenthes].carnivore.it
- www.honeyd.org
- www.honeypots-alliance.org.br
- isc.sans.edu/diary.html?storyid=7930
- www.malwaredomainlist.com
- www.rfc-editor.org
- www.hermano.com.br

OBRIGADO!

Perguntas?

seginfo@celepar.pr.gov.br

Produzido com:

debian GNOME

OpenOffice.org

INKSCAPE

GIMP

CELEPAR INFORMÁTICA do PARANÁ