

## Construção de ambiente de testes para detecção de invasões em redes de computadores.

Felipe Balabanian\*, Moisés Danziger, Prof. Marco Aurélio Amaral Henriques.

### Resumo

Construção de plataforma de simulação para estudo de botnets e sistemas de detecção utilizando-se Omnet++/Inet (Simulador de rede) com integração de ferramentas específicas como Matlab e JaCaMo.

### Palavras-chave:

segurança de redes, botnets, detecção de invasões.

### Introdução

Botnets podem se comportar como verdadeiras ameaças cibernéticas à globalização digital, uma vez que podem ser usadas para negar acesso a serviços online ou até mesmo roubar e destruir informações [1].

O principal objetivo deste projeto é a construção de um ambiente apropriado para a execução/simulação de invasões em redes de computadores causadas por botnets (equipamentos controlados remotamente com o intuito de invadir e/ou causar algum dano a outras redes de computadores). Tal ambiente deverá facilitar a experimentação aos pesquisadores, permitindo um melhor entendimento do funcionamento de botnets e a validação de novas abordagens de detecção e desarticulação [2].

### Resultados e Discussão

Este trabalho focou na construção de ferramentas que permitam simular botnets, sistemas de defesa e detecção em redes de computadores.

Para a realização da simulação de rede utilizou-se o framework Omnet++ (simulador de eventos discretos) com a biblioteca Inet especializada em protocolos de rede. Um exemplo de simulação Omnet++ é ilustrado na Fig.1.

Foram construídos diversos módulos adicionais que permitiram o estudo de botnets e de seus detectores. Entre eles um módulo que simula uma botnet genérica simples, um módulo de teste de conectividade (ping), um módulo de geração de tráfego de rede TCP, um módulo de captura de pacotes (sniffer), um módulo de detecção de intrusão (IDS) e um módulo de comunicação com programas externos como Matlab e JaCaMo (plataforma de agentes autônomos) para a realização de simulações e análises mais sofisticadas.

O módulo de botnet simula o ciclo de vida da botnet real, escaneando a rede, buscando vulnerabilidades, invadindo computadores vulneráveis, informando ao botmaster o sucesso da invasão e aguardando novas ordens.

A integração da plataforma com ferramentas poderosas como o Matlab permite a análise do cenário de simulação em tempo de execução pelos diversos recursos e gráficos disponibilizados pelas mesmas. Facilita-se assim a análise, visualização e controle da rede simulada, como ilustrado na Fig. 2.

A flexibilidade do ambiente criado permitiu também a integração deste com a plataforma de simulações de agentes inteligentes JaCaMo, abrindo caminho para a criação de experimentos com botnets mais sofisticadas, baseadas em técnicas de inteligência computacional [3].

Todos os módulos foram desenvolvidos neste trabalho utilizando a linguagem C++, base do próprio Omnet++, o que conferiu ao ambiente a velocidade e

escalabilidade desejadas. Para utilizar os módulos descritos, basta instalá-los com o Omnet++/Inet, disponível para ambientes Linux e Windows [4].

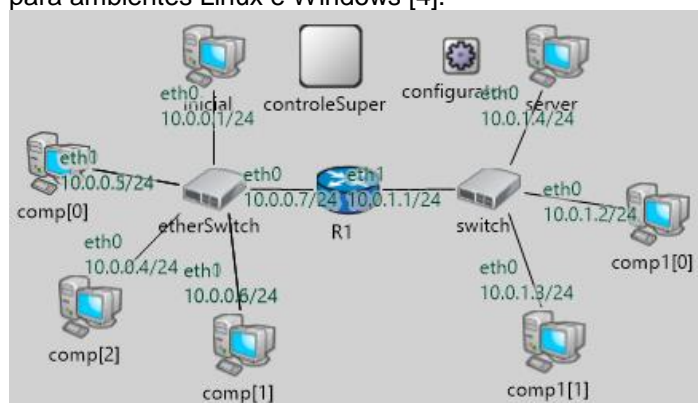


Figura 1: Rede simulada no ambiente Omnet++.



Figura 2: Análise via Matlab da comunicação entre o centro de comando da botnet e um computador infectado na rede da Figura 1.

### Conclusões

Neste trabalho foi possível criar e integrar módulos diversos em um ambiente de simulação para o estudo de botnets e de metodologias de detecção e prevenção das mesmas. Espera-se que este ambiente possa ser de grande utilidade para os pesquisadores que não dispõem de hardware suficiente para realizar experimentos de maior porte e/ou que demandem níveis de isolamento e segurança mais elevados.

### Agradecimentos

Este trabalho é parcialmente financiado pelo CNPq (Proc. Núm. 119785/2015-3).

[1] Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E. and Martini, P.; Botnets. SpringerBriefs in Cybersecurity, book. Springer, 2013.

[2] A. J. Aviv and A. Haeberlen, "Challenges in experimenting with botnet detection systems," in USENIX 4th CSET Workshop, San Francisco, CA, 2011.

[3] Moisés Danziger e Marco A. A. Henriques, Autonomous Bots - a disruptive element into botnet's scenario, submetido ao Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg 2016, Niterói, Brasil.

[4] Felipe Balabanian, Código-fonte dos módulos do simulador de botnets, <https://github.com/regras/simbo>.