doi:10.20396/revpibic.v0i0.id

Estudo sobre a aplicação de técnicas de inteligência computacional à área de segurança da informação

Fábio Harada Kubo*, Marco Aurélio Amaral Henriques

Resumo
Este trabalho teve como objetivo aprimorar o simulador Simbo, projetado para simulações de botnets que façam uso de novas técnicas de ataque baseadas no uso de aprendizado de máquina. Para alcançar esse objetivo, propusemos um cenário no qual os bots atuam no host infectado filtrando o tráfego da rede e reportando informações relevantes para seu centro de comando e controle que, dotado de um motor inteligente, é responsável pela tomada de decisões. A fim de melhorar também a escalabilidade do simulador, desenvolvemos uma solução para distribuir a simulação em vários núcleos de processamento, aumentando o desempenho do simulador. Esta solução permitirá o estudo de cenários maiores e mais complexos que os avaliados até o momento.

Palavras-chave:
Botnet, Simulação, Aprendizado de máquina

Introdução

Botnets (conjunto de computadores infectados com software que formam uma rede e podem ser usados para executar ações maliciosas) são considerados pragas virtuais que afetam milhões de usuários. Na guerra contra os botnets, o mercado de segurança da informação parece estar sempre um passo atrás. Desta forma, o estudo de novos modelos de botnet é uma maneira de ajudar no desenvolvimento de novas ferramentas de defesa. Neste sentido, o conteúdo deste trabalho baseia-se na melhoria do simulador de botnets Simbo, apresentado por Balabanian et al (2016), para permitir seu uso em simulações de botnets avançadas como as apresentadas por Danziger et al (2017). Tais botnets utilizam técnicas de aprendizado de máquina (ML) como um motor inteligente e não dependem mais do botmaster para suas tomadas de decisão.

Metodologia

Tomando como base a versão do simulador existente, passamos a desenvolver diversas melhorias para o mesmo de maneira a viabilizar novos e mais avançados experimentos com botnets dotadas de algum nível de inteligência. Foi mantida a plataforma base OMNeT++ e novos módulos foram desenvolvidos em C++ para atender os requisitos colocados pelos demais membros do grupo de pesquisa envolvidos com este tema. Em particular foram feitas atualizações nos módulos básicos e adotadas técnicas que permitissem uma execução paralela do simulador em várias CPUs, de modo a viabilizar simulações de maior porte em tempo aceitável.

Resultados e Discussão

O primeiro cenário avaliado é o de uma botnet com o motor inteligente no papel do botmaster. Neste protótipo, supõe-se que cada bot tem uma ferramenta de análise de rede, como Bro Network Security Monitor (Bro), que foi infectada e dominada por bots, e é responsável por capturar o tráfego de rede do host infectado, filtrá-lo e enviá-lo ao seu Centro de Comando e Controle (C2) controlado por um motor inteligente. Na tentativa de simular esse tráfego de rede, bases de dados obtidas da Web foram distribuídos da seguinte forma: um subconjunto de IPs é selecionado aleatoriamente como máquinas infectadas por bots, um cenário semelhante ao que uma botnet opera. Um problema detectado nessa fase foi a falta de escalabilidade para simulações com grande número de bots, já que os bancos de dados a serem filtrados possuem tamanhos consideráveis. Assim, seguindo o trabalho de Stoffer et al. (2014) foram feitas modificações no OMNeT ++ e no INET para permitir a distribuição da simulação em vários núcleos de processamento. A Tabela 1 mostra os resultados obtidos em um cenário com 10 sub-redes e 1000 hosts trocando mensagens simples com C2 dentro de uma hora.

Tabela 1. Tempo e speedup das simulações

# de processos	Tempo de Execução (s)	Speedup
1 processo	112.8 ± 7.8	1.00
2 processos	80.6 ± 5.9	1.40
3 processos	47.6 ± 8.9	2.37
4 processos	38.9 ± 5.8	2.90

Como podemos ver, essa nova funcionalidade levou a uma diminuição no tempo de execução da simulação, permitindo o aumento do número de hosts e/ou do processamento em cada host. Assim, as técnicas de inteligência computacional podem ser inseridas mais facilmente nos bots, transformando seu modus-operandi.

Conclusão

Os resultados demonstram que a versão melhorada do Simbo permite simular modelos de botnets maiores e mais complexos com mais eficiência, viabilizando estudos de botnets que utilizam ML no C2 ou nos bots.

Agradecimentos

Ao CNPq pela bolsa de incentivo à pesquisa no programa PIBIC.

Balabanian, F.; Danziger, M. e Henriques, M. A. A. Simbo – Ambiente de Simulação dedicado ao Estudo de Botnets. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 16., 2016, Niterói, *Anais...*, p. 606-610.

Danziger, M e Henriques, M. A. A. Attacking and defending with Intelligent Botnets. In: Simpósio Brasileiro de Telecomunicações e Processamento de Sinais, 35., 2017, São Pedro, Anais..., p. 457-461.

Stoffer, M. et al. Enabling Distributed Simulation of OMNeT++ {INET} Models, 2014. Disponível em: <http://arxiv.org/abs/1409.0994>. Acesso em 11 jun. 2018.