RESUMO

GONÇALVES, D. S. M. *Sistema de Proteção contra Ataques de Botnets usando Redes Definidas por Software*. 2020. 63 f. Dissertação (Mestrado em Engenharia Eletrônica) – Faculdade de Engenharia, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2020.

Os ataques de negação de serviço crescem a cada ano exigindo investimentos financeiros e tecnológicos por parte das corporações para evitar danos aos seus serviços prestados na Internet. Em geral, os sistemas de proteção contra esses ataques são implementados através de equipamentos caros que processam um alto volume de tráfego. Além disso, algumas empresas oferecem serviços de tratamento de tráfego malicioso destinado a outros sistemas autônomos na Internet que também são caros. Esta dissertação propõe um sistema de proteção contra ataques de *botnets* do tipo HTTP flood baseado na tecnologia de redes SDN (*Software Defined Networking*) utilizando a colaboração de outros ASs. Esses ASs utilizam redes SDN controladas através de uma VPN pelo sistema de proteção do servidor web alvo dos ataques. Uma outra VPN implementada é utilizada para permitir que os ASs colaboradores enviem requisições diretamente ao servidor web que encontra-se protegido pelo sistema original. As requisições destinadas ao servidor web com o serviço desejado são atendidas pelo sistema e recebem um redirecionamento para o destino real da aplicação protegida. Através da implementação do sistema com SDN, cada requisição terá um fluxo permissivo escrito em um comutador virtual que da acesso ao servidor web. Como as requisições das *botnets* não acessarão o destino real por não seguirem o redirecionamento recebido, apenas requisições de clientes legítimos alcançarão o servidor protegido. Isso permite ao sistema diferenciar IPs atacantes de IPs de clientes legítimos. Dessa forma, os atacantes são bloqueados através de fluxos de bloqueio inseridos no comutador virtual de entrada do sistema. O sistema proposto foi implementado e avaliações de desempenho foram realizadas. Os resultados obtidos mostram reduções gradativas no consumo de CPU do servidor do controlador local, durante um ataque, na medida que ASs colaboradores são adicionados ao sistema. Com seis ASs colaboradores e com o sistema sendo atacado, foram registradas uma queda de consumo de CPU do servidor do controlador local de 65,32%, uma queda de latência percebida pelos clientes de 6 s para aproximadamente 400 ms e uma queda no consumo de CPU do servidor web de 78%.

Palavras-chave: SDN. Ataques. Proteção.