INVESTIGANDO O USO DE COAP EM ATAQUES DRDOS [1]

Guilherme Roberto Utech [2], Rafael Rodrigues Obelheiro[3]

[1] Vinculado ao projeto "Análise e Caracterização de Tráfego DRDoS"
[2]Acadêmico (a) do Curso de Ciência da Computação – CCT – Bolsista PROBIC
[3] Orientador, Departamento de Ciência da Computação – CCT – rafael.obelheiro@udesc.br

Ataques distribuídos de negação de serviço por reflexão (*Distributed Reflection Denial of Service*, DRDoS) são ataques realizados pela Internet que visam saturar vítimas com tráfego de rede de modo a provocar a indisponibilidade de serviços e/ou da própria rede. Em um ataque DRDoS, o atacante envia tráfego para um servidor vulnerável, que responde enviando tráfego não para a real origem, mas para a vítima. Quando as respostas são maiores que as requisições, o que é frequente, o tráfego enviado pelo atacante é amplificado pelo servidor que age como refletor. Dentre os diversos protocolos que podem ser usados em ataques DRDoS, um dos mais recentes é o CoAP (*Constrained Application Protocol*), um protocolo inspirado no HTTP (*HyperText Transfer Protocol*) voltado à comunicação entre dispositivos com recursos computacionais limitados.

O objetivo deste trabalho era investigar o uso do CoAP em ataques DRDoS. Para isso, foi desenvolvido um *honeypot* específico para esse protocolo, que registra as requisições CoAP recebidas e envia uma resposta fixa, idêntica à resposta mais usada em ataques com CoAP. Para evitar que o *honeypot* contribua significativamente em ataques DRDoS, o número de respostas diárias por endereço de origem é limitado. O *honeypot* CoAP foi incorporado a um *honeypot* usado para a observação de ataques DRDoS que já contava com outros sete protocolos, e colocado em produção na rede da UDESC em março de 2020.

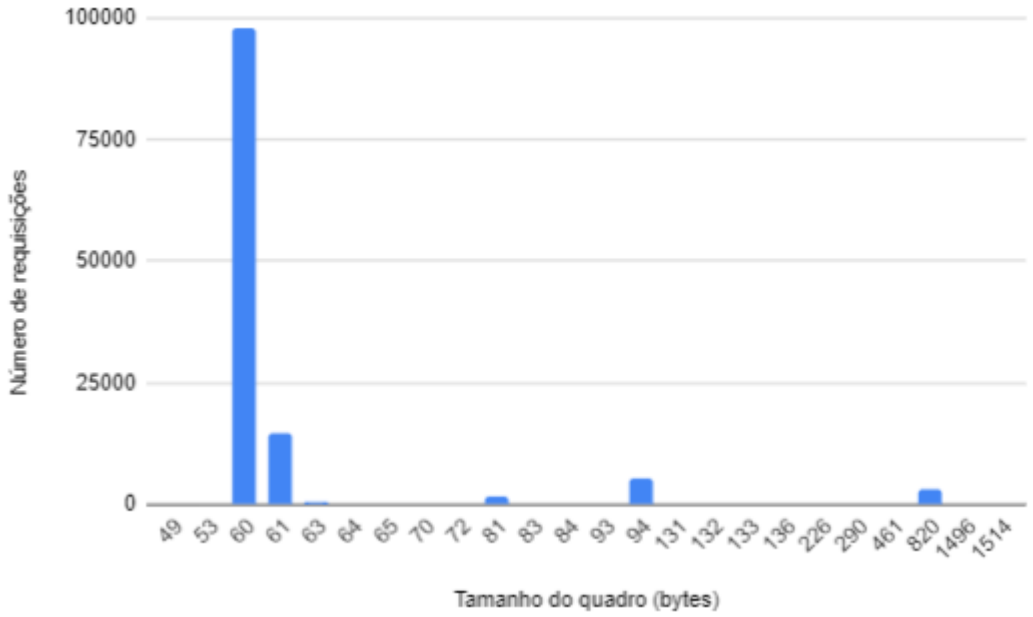
Foi realizada uma análise preliminar dos dados coletados pelo *honeypot* CoAP durante cinco meses, de 03/03 a 03/08. Nesse período foram recebidas 110.602 requisições, uma média de 737,3 requisições por dia. Considerando um ataque DRDoS como um conjunto de cinco ou mais requisições com endereços IP de origem pertencentes à mesma rede, em que requisições consecutivas têm um intervalo máximo de 60 segundos (definição usada no projeto de pesquisa), foram registrados apenas 28 ataques ao longo do período, correspondendo a 73.116 requisições (66,1% do total). O número de requisições por ataque ficou entre 5 e 24.823, tendo uma distribuição assimétrica à direita com mediana de 226. A duração dos ataques variou entre 2,0 e 104,9 segundos, com distribuição simétrica com média de 54,9 s. De forma geral, as estatísticas mostram que o *honeypot* observou um volume pequeno de ataques, os quais tiveram pouca intensidade e duração. Tipicamente, porém, o *honeypot* é apenas um dos vários refletores usados em ataques DRDoS, o que relativiza o baixo impacto dos ataques.

A Figura 1 mostra que 96,6% dos pacotes CoAP tiveram 60 ou 61 bytes de comprimento, o que corresponde a um fator de amplificação inferior a 25 para uma resposta de 1496 bytes. A análise do conteúdo mostrou que 109.998 requisições (99,5% do total) continham uma URI nula, e que 21

dos 28 ataques continham apenas requisições malformadas (isto é, com formatos que desviam da especificação do protocolo). Esses dados demonstram a intenção de minimizar o tamanho das requisições para assim maximizar a amplificação do ataque.

Pode-se concluir que o *honeypot* desenvolvido permite a observação de ataques DRDoS usando CoAP, e que esses ataques tiveram pouca relevância no período observado. Na continuidade da pesquisa, pretende-se ampliar a coleta de dados, aprofundar a investigação sobre o conteúdo dos pacotes e o uso do CoAP em ataques DRDoS multiprotocolo em conjunto com os demais protocolos suportados pelo *honeypot*.

Figura 1. *Distribuição de tamanho das requisições.*



Palavras-chave: DRDoS. CoAP. *Honeypot*.