Investigando o Uso de CoAP em ataques DRDoS

Guilherme R. Utech[1], **Rafael R. Obelheiro**[1]

[1]Departamento de Ciência da Computação
Universidade do Estado de Santa Catarina (UDESC), Campus Joinville

utech.br@gmail.com, rafael.obelheiro@udesc.br

Resumo. *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, causando assim a indisponibilidade de serviços e/ou da própria rede. Um dos protocolos mais recentes no cenários de DRDoS é o CoAP (Constrained Application Protocol), voltado a dispositivos IoT. Este trabalho descreve um honeypot desenvolvido para observar ataques DRDoS usando o CoAP, e apresenta uma análise preliminar de dados coletados pelo honeypot durante um período de cinco meses.*

1. Introdução

Ataques distribuídos de negação de serviço (*Distributed Denial of Service*, DDoS) estão presentes na Internet há cerca de 25 anos, e 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 [Mansfield-Devine 2015]. Ataques distribuídos de negação de serviço por reflexão (*Distributed Reflection Denial of Service*, DRDoS) são um tipo particular de ataque DDoS [Paxson 2001]. Em um ataque DRDoS, o atacante envia tráfego para um servidor vulnerável, que age como um refletor, enviando o tráfego de resposta não para a real origem, mas para a vítima do ataque. Quando as respostas são maiores que as requisições, o que é frequente, o tráfego enviado pelo atacante é amplificado pelo refletor. Fatores que concorrem para a popularidade de ataques DRDoS incluem a dificuldade de localizar os autores de ataques, a grande disponibilidade de refletores na Internet e a amplificação de tráfego, que permite que mesmo um atacante com recursos modestos consiga realizar ataques de grande intensidade [Heinrich et al. 2017].

Diversos protocolos podem ser utilizados em ataques DRDoS, usando tanto UDP como TCP como protocolo de transporte [Rossow 2014]. Um protocolo que passou a ser explorado recentemente é o CoAP (*Constrained Application Protocol*) [Shelby et al. 2014], um protocolo baseado em UDP voltado para a comunicação entre dispositivos na Internet das Coisas (*Internet of Things*, IoT). Relatos sobre o uso do CoAP em ataques DRDoS reportam um fator de amplificação de até 46, e ataques com tráfego médio de 55 Gbps e pico de 320 Gbps [Cimpanu 2018]. O crescimento da IoT deve induzir um aumento no número de dispositivos com suporte a CoAP conectados à Internet. Esse aumento, somado à dificuldade de garantir a segurança de dispositivos IoT [Boeckl et al. 2019], permite supor que este tipo de ataque seja cada vez mais comum no futuro.

A análise e caracterização do tráfego associado a ataques DRDoS é importante para entender como esses ataques efetivamente funcionam, e para orientar o

desenvolvimento de contramedidas [Heinrich 2019]. Embora existam diversos trabalhos na literatura devotados à análise e caracterização de tráfego DRDoS, como [Krämer et al. 2015, Noroozian et al. 2016, Heinrich et al. 2017, Thomas et al. 2017, Heinrich and Obelheiro 2019], nenhum deles considera o CoAP.

O objetivo deste trabalho é investigar o uso do CoAP em ataques DRDoS. Para isso, foi desenvolvido um *honeypot* específico para esse protocolo, que registra as requisições CoAP recebidas. Este artigo apresenta o *honeypot* e faz uma análise preliminar dos dados coletados entre março e agosto de 2020.

O restante deste artigo está organizado como segue. A Seção 2 dá uma visão geral do CoAP. A Seção 3 descreve o *honeypot* CoAP. A Seção 4 apresenta a análise dos dados. Finalmente, a Seção 5 conclui o artigo.

2. CoAP

O CoAP (*Constrained Application Protocol*) [Shelby et al. 2014] é um protocolo especializado em transferência web criado com o objetivo de ser usado em dispositivos com recursos computacionais limitados, no contexto de IoT. Inspirado no HTTP (*HyperText Transfer Protocol*), o CoAP é um protocolo requisição-resposta, sendo voltado para a transferência de dados M2M (*machine-to-machine*). O CoAP segue o princípio RESTful [Fielding 2000] para separar a API (*Application Programming Interface*) em recursos lógicos, e utiliza os métodos GET, POST, PUT e DELETE para manipulá-los.

Mensagens CoAP (tanto requisições como respostas) possuem um cabeçalho de 4 bytes, que pode ou não ser seguido de algumas opções binárias e um *payload*. O cabeçalho contém um identificador (*message-ID*) de 16 bits, usado para detecção de mensagens duplicadas e retransmissão de mensagens perdidas. Um *token* (opcional) pode ser usado para vincular requisições e respostas. Esse *token* é uma sequência de 0 a 8 bytes de comprimento gerada pelo cliente, e o servidor deve incluir em uma resposta o *token* da requisição correspondente. Os recursos disponíveis em um *host* CoAP são identificados por URIs (*Universal Resource Identifiers*), que são codificados nas opções do cabeçalho.

O uso do CoAP em ataques DRDoS é similar ao de outros protocolos baseados em UDP [Paxson 2001]. O atacante envia requisições CoAP para um dispositivo acessível na Internet; como as requisições têm IP de origem forjado, o tráfego de resposta é enviado para vítima [Netscout 2019].

A vulnerabilidade do CoAP a ataques DRDoS é reconhecida na especificação do protocolo [Shelby et al. 2014]. A RFC recomenda a utilização de DTLS (*Datagram TLS*) [Rescorla and Modadugu 2012] para a autenticação e autorização de pares. Quando o DTLS não está sendo utilizado, a RFC sugere o uso de *firewalls* para restringir o acesso externo aos dispositivos CoAP, e que respostas longas sejam fracionadas, diminuindo assim o fator de amplificação.

3. *Honeypot* CoAP

Para permitir a coleta e análise de dados de ataques DRDoS usando CoAP, foi desenvolvido *honeypot* específico para o protocolo. De maneira breve, um *honeypot* é uma ferramenta utilizada para observar o comportamento de usuários maliciosos; ele coleta dados quando usuários interagem com a ferramenta acreditando se tratar de um servidor vulnerável a fim de utilizá-lo para ataques [Hoepers et al. 2007].

O *honeypot* CoAP foi implementado usando Python e a biblioteca aiocoap.[1] O *honeypot* captura todo o tráfego CoAP recebido em formato PCAP, usando Tcpdump [TCPDUMP 2020], para posterior análise. O código Python contabiliza cada requisição e sintetiza uma resposta. A contabilização é feita em memória para propiciar eficiência, e os dados são posteriormente salvos em um banco de dados. Atualmente é sintetizada uma resposta fixa de 1496 bytes a uma requisição `GET ./well-known/core`, que é um URI usado para obter a descrição dos recursos de um dispositivo. Essa resposta foi escolhida por causa da sua predominância nos ataques descritos em [Netscout 2019] e para simplificar o processamento de requisições, dispensando uma lógica potencialmente complexa para tratamento de outros URIs. Os resultados da Seção 4 mostram que a simplificação não afeta o recrutamento do *honeypot* como refletor em ataques DRDoS.

O *honeypot* CoAP foi posto em produção em março de 2020 e está integrado a um *honeypot* já existente que conta com outros sete protocolos [Heinrich 2019]. Para evitar que o *honeypot* tenha uma contribuição significativa nos ataques que tentam utilizá-lo, o número de requisições diárias respondidas por IP é limitado: as requisições são registradas pelo *honeypot* mas não recebem resposta. Além disso, são bloqueadas respostas para requisições cujos endereços IP de origem são associados a projetos que varrem a Internet procurando por servidores vulneráveis (como [Cymru 2020] e [OpenNTP 2020]), evitando assim que o *honeypot* apareça nas listas produzidas por esses projetos. A relação de endereços IP bloqueados foi compilada de várias fontes (*e.g.*, [Mertens 2015], páginas web dos projetos), e é atualizada manualmente sempre que novos endereços são descobertos (durante análise manual de logs, por exemplo).

Para restringir a exposição do *honeypot*, o código fonte da ferramenta e os dados por ela coletados não estão disponíveis publicamente. No entanto, estamos dispostos a compartilhar a ferramenta com outros pesquisadores que estejam interessados.

4. Análise preliminar dos resultados

Foi realizada uma análise preliminar dos dados coletados pelo *honeypot* CoAP durante cinco meses, de 03/03/2020 a 03/08/2020. Nesse período foram recebidas 110.602 requisições, uma média de 737,3 requisições por dia. Para ser possível realizar uma investigação sobre ataque DRDoS utilizando CoAP vamos utilizar a seguinte definição de ataque DRDoS [Heinrich 2019]:

> *Considera-se 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.*

De acordo com essa definição, foram registrados apenas 28 ataques ao longo do período. Estes ataques tiveram um total de 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 segundos.

A Tabela 1 mostra que 91,2% das requisições 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. Esse fator é menor que os reportados anteriormente na literatura, de

[1] `https://github.com/chrysn/aiocoap`

46 [Cimpanu 2018] e 34 [Netscout 2019]. A análise do conteúdo mostrou que 109.998 requisições (99,5% do total) não continham um URI, e que 21 dos 28 ataques continham apenas requisições malformadas (isto é, com formatos que desviam da especificação do protocolo). Esses dados permitem inferir a intenção de minimizar o tamanho das requisições para assim maximizar a amplificação do ataque.

tamanho dos quadros (bytes)	requisições (%)
60	79,3
61	11,9
94	4,2
820	2,5
81	1,3
outros	0,8

Tabela 1. Distribuição do tamanho das requisições CoAP.

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. Outro fator que relativiza esse baixo impacto é que, excetuando-se o mês de junho, o número médio de requisições diárias segue uma tendência de alta, como mostra a Figura 1. É razoável supor que ao menos parte desse tráfego corresponde a varreduras (*scans*) em busca de refletores que possam ser usados para ataques DRDoS no futuro, gerando a expectativa de que o crescimento no volume de requisições continue. Com relação à redução no número de requisições em junho, ela é explicada em parte por um período de instabilidade na rede onde se encontra o *honeypot*, que o deixou inacessível. Essa indisponibilidade não explica toda a diminuição no volume de requisições, porém; dado que o *honeypot* apenas reage ao tráfego que recebe, é difícil deduzir o que além de variação aleatória na incidência de ataques pode ter provocado a redução observada.

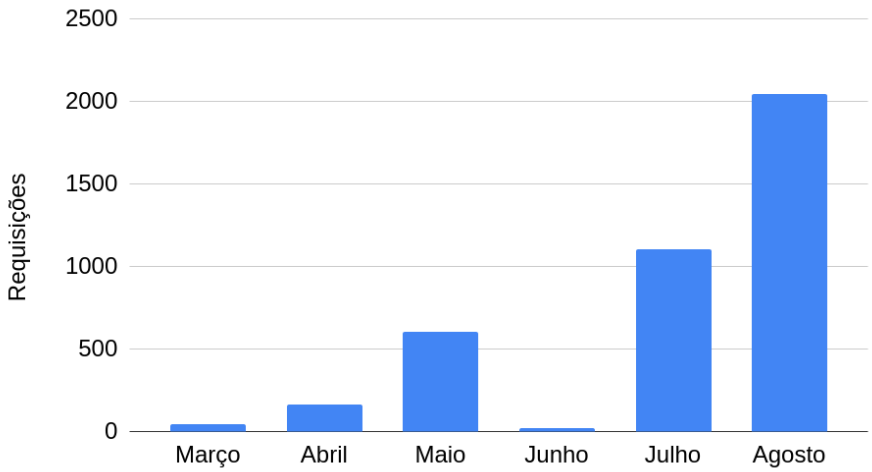

Figura 1. Média diária de requisições.

5. Conclusão

O CoAP é um protocolo relativamente recente no contexto de ataques distribuídos de negação de serviço por reflexão, e apresenta uma tendência de crescimento devido a seu uso em dispositivos IoT. Este trabalho apresentou um *honeypot* CoAP desenvolvido para permitir a observação e caracterização desses ataques. A análise preliminar dos dados coletados em um período de cinco meses mostrou, por um lado, um número ainda pequeno de ataques com baixa intensidade, e, por outro, um crescimento no tráfego CoAP observado pelo *honeypot*.

Na continuidade da pesquisa, iremos prosseguir com a coleta de dados com o *honeypot* e aprofundar a análise sobre os conteúdos das mensagens e suas particularidades. Pretende-se também realizar uma investigação sobre o uso do CoAP como mais um de vários outros protocolos utilizados em ataque multiprotocolo [Heinrich 2019].

Referências

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K., Nadeau, E., Piccarreta, B., O'Rourke, D. G., and Scarfone, K. (2019). Considerations for managing internet of things (IoT) cybersecurity and privacy risks. NISTIR 8228, NIST. `https://doi.org/10.6028/NIST.IR.8228`.

Cimpanu, C. (2018). The CoAP protocol is the next big thing for DDoS attacks. ZDNet. `https://zd.net/333hymy`.

Cymru (2020). DNS research at Team Cymru. `http://dnsresearch.cymru.com/`.

Fielding, R. (2000). *Architectural Styles and the Design of Network-based Software Architectures*. PhD thesis, University of California, Irvine.

Heinrich, T. (2019). Caracterização de Ataques DRDoS Usando Honeypot. Dissertação de mestrado em Computação Aplicada, UDESC, Joinville (SC).

Heinrich, T., Longo, F. S., and Obelheiro, R. R. (2017). Experiências com um honeypot DNS: Caracterização e evolução do tráfego malicioso. In *XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*.

Heinrich, T. and Obelheiro, R. R. (2019). Brasil vs mundo: Uma análise comparativa de ataques DDoS por reflexão. In *XIX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*.

Hoepers, C., Steding-Jessen, K., and Chaves, M. (2007). Honeypots e honeynets: Definições e aplicações. `http://www.cert.br/docs/whitepapers/honeypots-honeynets/`.

Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., and Rossow, C. (2015). AmpPot: Monitoring and defending against amplification DDoS attacks. In *International Workshop on Recent Advances in Intrusion Detection*, pages 615–636. Springer.

Mansfield-Devine, S. (2015). The growth and evolution of DDoS. *Network Security*, 2015(10):13–20.

Mertens, X. (2015). Port scanners: The good and the bad. https://bit.ly/3lQmFNF.

Netscout (2019). CoAP attacks in the wild. ASERT blog, https://www.netscout.com/blog/asert/coap-attacks-wild.

Noroozian, A., Korczyński, M., Gañan, C. H., Makita, D., Yoshioka, K., and van Eeten, M. (2016). Who gets the boot? analyzing victimization by DDoS-as-a-Service. In *International Symposium on Research in Attacks, Intrusions, and Defenses*, pages 368–389. Springer.

OpenNTP (2020). OpenNTPProject.org – NTP scanning project. http://openntpproject.org/.

Paxson, V. (2001). An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communication Review*, 31(3):38–47.

Rescorla, E. and Modadugu, N. (2012). Datagram transport layer security version 1.2. RFC 6347. https://tools.ietf.org/html/rfc6347.

Rossow, C. (2014). Amplification hell: Revisiting network protocols for DDoS abuse. In *Network and Distributed System Security Symposium (NDSS)*.

Shelby, Z., Hartke, K., and Bormann, C. (2014). The constrained application protocol (CoAP). RFC 7252. https://tools.ietf.org/html/rfc7252.

TCPDUMP (2020). TCPDUMP/LIBPCAP public repository. https://www.tcpdump.org/.

Thomas, D. R., Clayton, R., and Beresford, A. R. (2017). 1000 days of UDP amplification DDoS attacks. In *APWG Symposium on Electronic Crime Research (eCrime)*, pages 79–84. IEEE.