Ataques DDoS em Dispositivos IoT: Funcionamento, Impactos e Medidas de Prevenção

Franklin Matias Engelmann, Angelo Elias Dal Zotto

RESUMO

Este trabalho analisa os ataques de negação de serviço distribuídos (DDoS) no contexto da Internet das Coisas (IoT), destacando como dispositivos vulneráveis podem ser explorados por invasores. São descritos os principais tipos de ataques, como HTTP Flood, SYN Flood, ICMP Flood, Reflexão/Amplificação e SlowLoris, evidenciando suas técnicas e impactos na indisponibilidade de serviços críticos. O estudo também apresenta o caso do Mirai Botnet, que em 2016 demonstrou o potencial destrutivo de milhares de dispositivos IoT comprometidos em um ataque coordenado de larga escala. Além disso, discute medidas preventivas, como alteração de senhas padrão, atualização constante de firmware, autenticação em dois fatores e uso de firewalls, ressaltando que a segurança é responsabilidade conjunta de fabricantes e usuários. Conclui-se que, diante da expansão contínua da IoT, a conscientização e boas práticas de proteção são essenciais para reduzir riscos e mitigar novos ataques.

Palavras-chave: IoT. Ataques DDoS. Botnet. Segurança da Informação.

1 INTRODUÇÃO

Este trabalho irá descrever o funcionamento de um ataque de DDoS (*Distributed Denial of Service*) que utiliza dispositivos IoT como o seu vetor de ataque e apresentar uma contextualização dos conceitos envolvidos e uma pesquisa bibliográfica de tais ataques.

O termo “Internet das Coisas” (IoT – *Internet of Things*, em inglês) apareceu pela primeira vez em 1999 em um artigo de Kevin Ashton, representando que todos os dispositivos podem estar conectados à internet (PROPMARK, 2021).

2 FUNDAMENTAÇÃO TEÓRICA

Um ataque DoS (Denial of Service) tem a intenção de gerar negação de serviço por meio de sobrecarga de comunicação ou de processamento do alvo do ataque. Uma negação de serviço é um ataque cibernético que tem como objetivo tornar um sistema, servidor ou serviço indisponível para seus usuários legítimos. Como os alvos de um DoS são normalmente servidores web, esse ataque provoca inacessibilidade do sistema. Um ataque de DDoS é um ataque distribuído de negação de serviço, sendo mais sofisticado por distribuir a carga de ataque entre vários dispositivos. No DDoS, vários dispositivos infectados mantêm inúmeras solicitações para o alvo. Segundo Fraga (2019, p. 329), “esse ataque [DDoS] tem sido mais utilizado atualmente devido às infraestruturas de muitos alvos deste ataque (sites governamentais, bancários, políticos e servidores de jogos online) possuírem configurações de prevenção de alta tecnologia”.

Existem diversos tipos de ataque de DDoS. Este trabalho irá abordar alguns deles e como funcionam, como por exemplo HTTP Flood, SYN Flood, ICMP, Reflexão e Amplificação e SlowLoris.

HTTP Flood tem como alvo servidores e aplicativos web. O ataque utiliza botnets para fazer envio de grandes volumes de dados para o servidor responder.

Um botnet é a junção de duas palavras, abreviação da palavra robot (bot) que significa robô e network (net), desta forma, botnet significa uma grande quantidade de robôs conectados à rede (GOGONI, 2020). As solicitações do HTTP Flood podem ser de scripts, imagens ou POSTs HTTP. Quando acontecem inúmeras requisições, o servidor aloca o máximo de recursos disponíveis para poder atender. Desta forma, depois de certa quantidade de requisições, ele deixa de responder (FRAGA, 2019).

SYN Flood funciona de forma semelhante ao HTTP Flood, utilizando um pacote SYN (sincronização) do protocolo TCP, porém com o endereço de IP do atacante mascarado. O SYN realiza uma solicitação ao servidor para fazer uma conexão, o que faz com que ele acabe alocando alguns recursos para atender à demanda. Porém, essa solicitação é falsa e nunca será respondida pelo atacante. Quando o servidor aloca algum recurso, também existe um Time To Live (TTL), ou seja, um limite de tempo, para desalocar esse recurso. Porém, como os recursos são limitados, os usuários que utilizarem o serviço nunca conseguirão realizar alguma solicitação ao servidor por ele estar totalmente ocupado pelo ataque, sendo apenas liberado quando o ataque terminar, expirando o TTL das conexões do ataque (FRAGA, 2019).

O ICMP (Internet Control Message Protocol) é um protocolo utilizado para envio de mensagens de controle e diagnóstico em redes, como no comando ping. Quando explorado de forma maliciosa, pode ser usado como um ataque para negação de serviço, como o ping flood, que é um ataque que utiliza os pacotes “echo request” do ICMP para atingir o limite de requisições que um servidor pode atender. Para isso,o atacante necessita de uma conexão mais rápida que o servidor, com um tempo de resposta menor. Se o servidor for sobrecarregado de requisições, o mesmo se tornará irresponsivo (FRAGA, 2019).

Um ataque de reflexão e amplificação consiste no envio de informações de forma mascarada para vários computadores. Como esse ataque modifica as informações da conexão, o servidor passa a entender que o IP de uma requisição é o mesmo IP de origem. Dessa forma,as respostas às requisições são direcionadas ao próprio servidor. (FRAGA, 2019).

SlowLoris é um ataque lento e de baixa taxa de tráfego. Esse ataque deixa as requisições em aberto e faz com que o servidor guarde os recursos para uma requisição que nunca será concluída (FRAGA, 2019).

3 METODOLOGIA

Adotou-se uma pesquisa qualitativa, de caráter exploratório e descritivo, fundamentada em revisão bibliográfica. Foram consultados livros e publicações em meios digitais com o objetivo de compreender o funcionamento dos ataques de negação de serviço distribuídos (DDoS) no contexto da Internet das Coisas (IoT). A pesquisa qualitativa foi escolhida por permitir a análise interpretativa dos conceitos e fenômenos envolvidos, sem a necessidade de quantificação estatística, possibilitando a construção de um panorama teórico consistente sobre os tipos de ataques e seus riscos.

4 APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS

Observa-se uma tendência de aumento nos casos de servidores e sites que se tornam alvos de ataques DDoS realizados por meio de botnets de dispositivos IoT. De acordo com Pacecho & Yoachimik (2025), somente no segundo trimestre de 2025 foi registrado um crescimento de 44% no número de ataques em comparação ao mesmo período do ano anterior, demonstrando a gravidade dessa evolução. Tal cenário decorre, em grande parte, da busca por automação para facilitar a vida cotidiana, o que, quando mal administrado, gera vulnerabilidades significativas. Isso indica que dispositivos IoT, apesar de sua utilidade, podem representar riscos de segurança quando não configurados ou protegidos adequadamente.

Frequentemente, observa-se a aquisição de equipamentos de baixo custo ou até mesmo de versões similares aos modelos originais. Um exemplo é manter a senha padrão de um dispositivo. Caso o dispositivo fique com a senha padrão, ele pode facilmente ser invadido e ser usado como um dispositivo em uma botnet.

Um botnet muito usado para ataques a partir de IoT é o Mirai Botnet. Segundo Silveira (2020, p. 22), “Naquele ano [2006], quatrocentos mil dispositivos, incluindo câmeras e roteadores sem fio, infectados pelo malware Mirai formaram uma grande botnet que paralisou a Internet com um ataque DDoS orquestrado, estabelecendo um novo recorde de tráfego associado a um único evento (apud VLAJIC & ZHOU, 2018)”. O sistema IoT é utilizado para botnets pela sua fragilidade na parte de segurança, tornando esse um alvo de pesquisa em segurança da informação (SILVEIRA, 2020).

Por se tratar de um tipo de malware, a infecção pode ocorrer a partir da instalação de softwares pelo próprio usuário, por acessos secundários explorando vulnerabilidades de segurança ou, em alguns casos, já estar presente no equipamento adquirido, como foi identificado em determinados modelos de TV Box (ANATEL, 2025). Após a infecção, o malware pode permanecer inativo até que seja acionado por seu operador, o que dificulta sua detecção pelo usuário.

5 CONCLUSÃO

Maneiras de se prevenir para esta invasão e mitigar o problema que pode evoluir para um cenário global envolvem comprar equipamentos legítimos e com procedência, alterar todas as senhas padrões, usar duplo fator de autenticação ao vincular alguma conta para serviços sempre que possível, manter os sistemas atualizados e fazer a utilização de firewall.

Em conclusão, existem diversos tipos de ataques, com impactos diferenciados e situações diversas. A segurança da informação depende não somente dos desenvolvedores de dispositivos IoT, mas também do usuário final.

6 REFERÊNCIAS

FRAGA, Bruno. **Técnicas de Invasão – Aprenda as técnicas usadas por hackers em invasões reais.** Editora Labrador, 2019.

INFORCHANNEL. ***O malware mais procurado de fevereiro 2020: Mirai Botnet.*** Inforchannel, 20 mar. 2020. Disponível em: <https://inforchannel.com.br/2020/03/20/o-malware-mais-procurado-de-fevereiro-2020-aumento-de-ameacas-espalhando-o-mirai-botnet-para-dispositivos-de-iot/>. Acesso em: 19 de set. de 2025.

SILVEIRA, Frederico Augusto Fernandes. ***Smart-IoT: um sistema de proteção contra DDoS para rede de Internet das Coisas***; repositório UFRN, 2020. Disponível em: <https://repositorio.ufrn.br/bitstream/123456789/30831/1/SmartIoTsistema_Silveira_2020.pdf>. Acesso em: *19 de set. de 2025*.

GOGONI, Ronaldo. ***O que são botnets?***. Disponível em: <https://tecnoblog.net/responde/o-que-sao-botnets/>. Acesso em: *19 de set. de 2025*.

PROPMARK. ***Internet das coisas – a origem e o futuro da tecnologia que está mudando o mundo.***. Disponível em: <https://propmark.com.br/internet-das-coisas-a-origem-e-o-futuro-da-tecnologia-que-esta-mudando-o-mundo/#:~:text=“Internet%20das%20coisas”%20(ou,identificação%20de%20produtos%20por%20radiofrequência.>. Acesso em: *20 de set. de 2025*.

PACHECO, Jorge; YOACHIMIK, Omer. ***Hyper-volumetric DDoS attacks skyrocket: Cloudflare’s 2025 Q2 DDoS threat report.*** Cloudflare Blog, 15 jul. 2025. Disponível em: <https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/>. Acesso em: 20 de set. de 2025.

ANATEL. ***Anatel e PF desarticulam esquema milionário de “TV Box” e “Gatonet” em Operação PRAEDO.*** Brasília, 29 jul. 2025. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-e-pf-desarticulam-esquema-milionario-de-tv-box-e-gatonet-em-operacao-praedo>. Acesso em: 20 de set. de 2025.