Análise a Ataques *Distributed Denial-of-Service*

Ricardo Pereira, André Filho

***Resumo*—Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.**

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

***Palavras-chave*—IEEE, IEEEtran, journal, LaTeX, paper, template.**

I. Introdução

NUMA sociedade contemporânea que apresenta um aumento progressivo da sua interconetividade, os ataques *Distributed Denial-of-Service* (DDoS) prosseguem a representar uma das ameaças mais significativas, nomeadamente no âmbito destrutivo, ao quadro global da cibersegurança.

Neste seguimento, cabe notar que um ataque DDoS consiste, essencialmente, numa tentativa maliciosa de causar disrupção, por vezes total, na disponibilidade de um sistema alvo, nomeadamente servidores, serviços e redes, mediante a utilização de processos e ferramentas que possibilitam a sobrecarga deste mesmo ou da sua infraestrutura adjacente com uma desproporcionada enchente de tráfego irrelevante [1], [2]. Apesar destes ataques serem abrangidos pela categoria de ofensivas de *Denial-of-Service* (DoS), estes distinguem-se dos demais, principalmente, pela sua natureza distribuída, ou seja, mediante a utilização de diversos dispositivos eletrónicos, principalmente computadores, dispositivos *Internet of Things* (IoT) e outros aparelhos que possuam ligações à Internet, de modo a orquestrar um ataque coordenado que almeja promover no seu alvo um grau de inacessibilidade significativo, prejudicando, consequentemente, os seus utilizadores legítimos [3].

Assim, importa realçar que a constituição de uma rede de dispositivos eletrónicos que possam ser empregues numa ofensiva DDoS representa a generalidade de ataques deste tipo, sendo esta, frequentemente, realizada mediante a infeção de sistemas vulneráveis com diferentes categorias de *malware*. Estes sistemas, uma vez comprometidos, podem ser controlados remotamente pelo atacante, passando a ser designados como *bots* e, consequentemente, integrando uma *robot network* (BOTNET), podendo ser empregues pelo atacante como uma fonte de tráfego irrelevante. Nesta senda, cabe notar que a constituição de uma BOTNET possibilita que o atacante aumente a capacidade disruptiva do seu ataque, assim como dificulte a identificação da origem deste, uma vez que, para o sistema alvo, mais especificamente, os seus processos e ferramentas de proteção contra ataques DDoS, existem inúmeras fontes de tráfego distintas, minimizando a capacidade destes últimos localizarem com elevado grau de precisão o dispositivo coordenador do ataque [1].

A proteção dos sistemas supramencionados contra ataques DDoS revela-se imperativa, de modo a assegurar, principalmente, a sua disponibilidade, mas, também, a sua integridade. Os impactos de um ataque DDoS bem-sucedido numa organização podem afetar diversos âmbitos distintos desta, nomeadamente a sua reputação, os seus recursos financeiros, assim como a sua relação com os seus próprios funcionários e com os seus clientes, já que estes podem se encontrar privados, respetivamente, de realizarem as suas tarefas laborais e de acederem aos serviços prestados pela empresa [4].

Importa realçar que existe uma ampla variedade de indivíduos e entidades empresariais envolvidas em ataques DDoS, mais especificamente no horizonte ofensivo destes, assim como no defensivo. Deste modo, as motivações empregues na execução de ataques DDoS são, também, vastas, complicando, consequentemente, a identificação de intuitos concretos que possam ser associados a estes. Contudo, é possível reconhecer que, frequentemente, os ataques DDoS são realizados visando obter ganhos financeiros ou de causar o máximo de disrupção possível aos sistemas alvo, de modo a marcar posições e a viabilizar ações de *hackvism* [5].

No caso concreto do ano de 2024, os ataques DDoS apresentaram um crescimento de ocorrências. Existem diversos fatores que contribuíram para este aumento, nomeadamente a realocação de uma quantidade substancial de infraestrutura critica para o ambiente *online*, assim como a amplificação da cifra de dispositivos IoT que, por norma, possuem a ausência de proteções de segurança robustas, sendo a sua infeção com *malware* e consequente integração numa BOTNET facilitada [6].

Este documento visa clarificar o leitor sobre os ataques DDoS, mediante a facultação de informação concisa e relevante sobre a temática. Nesta senda, cabe realçar que foi, também, realizado uma demonstração prática sobre a constituição de uma BOTNET, assim como a execução de um ataque DDoS, mediante a utilização desta, de modo a ilustrar, de forma mais tangível, o funcionamento destes ataques e a

R. Pereira e A. Filho estão com o Instituto Politécnico de Leiria.

sua capacidade disruptiva.

Cumpre, ainda, esclarecer a estrutura do presente documento. Este relatório encontra-se organizado em 6 capítulos. Inicialmente é efetuada uma introdução ao contexto do problema, mais especificamente aos ataques DDoS. O segundo capítulo, procura proporcionar uma visão global sobre a temática, acrescentando detalhes cruciais à informação facultada no capítulo anterior, assim como abordando os mecanismos empregues pelos atacantes, aquando da constituição e execução de um ataque DDoS. No terceiro capítulo é efetuada uma abordagem à demonstração prática elaborada. O quarto capítulo procura facultar informação relevante no âmbito das estratégias e desafios de mitigação de ataques DDoS. No quinto capítulo, procura-se proporcionar uma perspetiva futura global sobre os ataques DDoS. Por fim, o documento termina com uma breve conclusão sobre a temática.

II. Panorama global

Tópicos a abordar (overview):

- 1 página
- Falar de uma maneira mais especifica sobre como se caracteriza cada ataque DDoS (coisas que os fazem unicos; tipos)
- como detetar um ataque (possivelmente aqui)
- Falar de motivacoes para fazer ataques DDoS (caracterizando-as: ganhos financeiros, ativismo; agenta politica; vandalismo: ect)
- Mencionar em maior detalhe os seus impactos (consequencias diretas e indiretas, como perdas financeiras, danos reputacionais, disrupcoes de infraestrutura critica)

Tópicos a abordar (mecanismo):

- 1 página
- Técnicas de amplfiuicação de tráfico (DNS, NTP, SNMP, SSDP, ect)
- Técnicas de exaustão de recursos (SYN flood, ACK flood, ect)
- Introduzir o conceito de botnets (o que sao; como sao criadas; como sao utilzadas; dar exemplos de botnets reais)
- Mencionar ferramentas e plataformas utilizadas para lançar ataques DDoS

III. Demonstração Prática

Tópicos a abordar:

- 0.75 paginas
- Setup
- Execução
- Resultados (e potenciais observações)
- Considerações éticas e legais (caso seja necessário palha)

IV. Estratégias e desafios na mitigação

Tópicos a abordar:

- 2 páginas
- Difiuldades de deteção
- Escalabilidade das defesas
- Sofisticação dos ataques
- Assimetria entre recursos de ataque e defesa (...)
- como detetar um ataque DDoS
- Estrategias de ultima geração com grandes impactos
- AI-Driven trafic analysis; cloud-based mitigation; zero-trust network security; ect
- Estrategias mais tradicionais e ferramentas (maybe)

V. Perspetiva futura

Tópicos a abordar:

- 1 página
- Evolução dos vetores de ataque
- Riscos associados à interconetividade de dispositivos (e de que maneira o aumento desta pode provocar mais problemas no ambito relevante)
- enfatizar o papel das redes 5g da escala enorme de interconetividade dos dispositivos
- O papel da IA e do ML na constituição de ataques DDoS e na proteção destes
- Politicas e regulamentações (caso seja necessaria palha)

VI. Conclusão

The conclusion goes here.

- 0.5-1 páginas

Referências Bibliográficas

[1] "What is a distributed denial-of-service (DDoS) attack?" [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[2] "What Is a DDoS Attack? | IBM," Oct. 2022. [Online]. Available: https://www.ibm.com/think/topics/ddos

[3] "DoS and DDoS Attacks. What are Their Differences? - zenarmor.com," Aug. 2024. [Online]. Available: https://www.zenarmor.com/docs/network-security-tutorials/dos-vs-ddos-attacks

[4] "Distributed Denial of Service: How DDoS Attacks Work," Jun. 2018, section: Pre-emptive Safety. [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work

[5] "What is a DDoS Attack? DDoS Meaning, Definition & Types." [Online]. Available: https://www.fortinet.com/resources/cyberglossary/ddos-attack

[6] L. Arnold, "The Rise of DDoS Attacks: A Growing Threat to Cyber Security," Sep. 2024. [Online]. Available: http://www.redhelix.com/media/ddos-attacks/

PLACE PHOTO HERE

Ricardo Pereira Biography text here.

André Filho Biography text here.