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. O conceito de BOTNET será posteriormente explanado detalhadamente no subcapítulo II.A. 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,

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

de forma mais tangível, o funcionamento destes ataques e a 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

Os ataques DDoS são uma ameaça informática frequentemente empregue, de modo a comprometer, principalmente, a disponibilidade de serviços, servidores, aplicações e redes. Neste seguimento, cabe notar que, estes ataques, possuem diversas características que os tornam únicos no âmbito dos ataques informáticos, mas, também, na categoria das ofensivas de DoS, nomeadamente na metodologia e ferramentas empregues para a sua concretização.

A. Conceito de BOTNET

Uma BOTNET é, na sua essência, uma rede de dispositivos eletrónicos sequestrados, mediante a utilização de diversas categorias de *malware*, por um atacante, de modo a possibilitar a realização de um ataque de negação de serviço em ampla escala, mas também de ataques de *phishing* e de *brute force*. Nesta senda, os dispositivos que compõem uma BOTNET são, principalmente, computadores, servidores, routers, câmaras de vigilância, e diversos outros aparelhos, nomeadamente dispositivos IoT. Assim, aquando da sua infeção, o atacante consegue, remotamente, controlar estes aparelhos, frequentemente sem o conhecimento e autorização dos seus proprietários. Estas redes revelam um elevado grau de distributividade e tolerância a falhas, multifuncionalidade, assim como persistência e inteligencia [7], [8].

No âmbito do funcionamento das BOTNETs, importa realçar que estas são construídas com base na sua futura expansão e automatização, assim como de modo a possibilitar amplificação da potencia e da velocidade de ataques de larga escala. Deste modo, um dispositivo pertencente a esta rede, denominado por *zombie* ou *bot*, é controlado, via instruções remotas, por um dispositivo central, sobre o total dominio do atacante, designado por *bot herder*. Nesta senda, cabe, também, notar que estas redes possuem um potencial imensamente destrutivo, já que são frequentemente vendidas ou alugadas, pelo seu criador, a indivíduos ou entidades, de modo a concretizar uma ou mais das diversas motivações inframenciondas [7], [8].

Neste seguimento, o atacante, via o dispositivo *bot herder*, emprega a estratégia de *Command-and-control* que permite, mediante a utilização de um servidor central, faculta a transmissão de instruções, remotamente, aos *bots* pertencentes à BOTNET, seguindo, também, modelos de comunicação centralizados, nomeadamente o paradigma *client-server*, ou descentralizados, principalmente o tipo *peer-to-peer*.

No caso concreto do modelo centralizado, cabe notar que este é organizado hierárquicamente, ou seja, existe um servidor central que possuí a função de transmitir todos os comandos aos *bots* podendo, também, existir intermediários entre a cimeira e a base da hierarquia denominados por *sub-herders* ou *proxies*. Por sua vez, os modelos descentralizados, atribuem a responsabilidade de transmissão de instruções a todos os dispositivos da BOTNET, inclusivamente os próprios *bots*, já que, basta o *bot herder* conseguir enviar os comandos para um dos *bots* para que estas sejam transmitidas a todos os elementos da rede em questão. Nesta senda, importa, ainda, realçar que o modelo descentralizado possuí, atualmente, uma maior ocorrência, dado que este permite uma ofuscação superior do atacante, assim como do *bot herder* [7].

Releva, ainda, notar que, posteriormente à infeção, o *bot* permite ao atacante, mais especificamente, acesso a operações *admin-level*, nomeadamente a leitura e escrita de dados de sistema, coleta de informação pessoal do proprietário, envio de dados, monitorizamento das atividades do utilizador, procura por vulnerabilidades e a instalação e execução de qualquer aplicação [7].

Assim, a construção de uma BOTNET pode ser organizada em 3 fases distintas, a saber:

- Preparação e Exposição: o atacante, incialmente, procura por uma vulnerabilidade num dos tipos de dispositivos supramencionados, visando descobrir uma falha que possibilite uma infeção sem rastro deste mesmo dispositivo [7].
- Infeção: o utilizador, ao executar uma ação, compromete o seu próprio dispositivo com o *malware* do atacante, tornado este num *bot*. Nesta senda, cabe notar que existem diversas formas de concretizar a infeção, nomeadamente via estratégias de *social engineering*, mas também mediante outras técnicas mais agressivas, principalmente o caso dos *drive-by downloads* [7].
- Ativação: o atacante possuí controlo total do *bot*, procedendo à sua adição à rede de BOTNET e, posteriormente, à sua utilização num ataque de negação de serviço, *phishing* ou *brute force* [7].

No âmbito de motivações, releva realçar que estas redes são frequentemente empregues em ações de furtos de fundos monetários e de informação pessoal, assim como outros tipos de esquemas, revelando curialidade à técnica de extorsão e a diversas práticas de roubo, assim como na constituição de esquemas. Além disso, são, também, utilizadas na sabotagem de serviços, já que estas possuem a capacidade de concretizar ataques DDoS poderosos [7].

B. Categorias de ataques DDoS

A categorização das distinções entre ataques DDoS permite aprimorar a compreensão que indivíduo possuí destes. Nesta

seda, cabe notar que existem 3 categorias principais de ataques de DDoS, a saber: *Volumetric DDoS Attacks*;*Protocol Attacks*; *Application Attacks* [9], [10].

As 3 categorias supramencionados facilitam a caracterização da grande parte de ataques DDoS. Contúdo, nem todos os ataques de negação de serviço em ampla escala podem ser balizados nas categorias definidas, principalmente ataques *Advanced Persistent* DoS, ataques que emprega múltiplos vetores e ataques DDoS *Zero-Day*. Assim, os atacantes empregam, frequentemente, uma combinação de técnicas e métodos distintos, de modo a fortalecer a robustez dos seus ataques, viabilizando a continuação do seu impacto, já que estes se tornam considerávelmente mais complicados de detetar e mitigar [9], [10].

1) Volumetric DDoS Attacks

No caso concreto dos ataques DDoS volumétricos, cabe notar que estes procuram sobrecarregar a capacidade de recursos de um dispositivo alvo, mediante utilização de um elemento curial a este processo, nomeadamente pedidos, tráfego e chamadas a, respetivamente, servidores, redes e bases de dados. Nesta senda, um ataque volumétrico de negação de serviço distribuída permite saturar a largura de banda do alvo, sendo a magnitude do ataque medida em *bits* transmitidos por segundo. Assim, releva realçar que os *Volumetric DDoS Attacks* incluem os diversos ataques de *flooding* inframencionados, nomeadamente *User Datagram Protocol* (UDP) *Flooding*, CharGEN *Flooding* e Internet Control Message Protocol (ICMP) *Flooding*, assim como ataques que empregam aplicações indevidamente utilizadas [9].

Neste seguimento, os ataques de UDP *Flooding* procuram enviar uma cifra desproporcionada de pacotes UDP ao alvo, de modo a sobrecarregar a sua capacidade de processamento destes mesmos, assim como exaustar a sua largura de banda. Assim, cabe notar que este ataque procura explorar a natureza do protocolo UDP, mais especificamente, a sua característica de não ser estabelecida uma conexão entre o emissor e o recetor, sendo apenas efetuada uma tentativa de envio do pacote, sem qualquer tentativa de obter uma resposta. Deste modo, os atacantes visam servidores presentes na Internet ou numa rede, via os seus endereços *Internet Protocol* (IP) e as portas associadas ao protocolo UDP [9]. Importa, ainda, realçar que este ataque incluí as variantes UDP *Fragmentation Flooding* e *Specific* UDP *Amplification Attacks*. A primeira variante, procura enviar pacotes UDP fragmentados de superior dimensão, visando que o alvo, ao receber estes e aquando do consequente processo de junção de fragmentos, fique sobrecarregado. Por sua vez, a segunda variante, procura enviar um único pedido UDP verdadeiro,utilizando o endereço IP do alvo, para diversos servidores, de modo a que estes respondam ao alvo e, consequentemente, promovam uma sobrecarga neste. Nesta senda, cabe notar que são empregues diversos protocolos que utilizam o modelo UDP, de modo a concretizar este ataque específico, a saber: Network Time Protocol; Simple Network Management Protocol; e Simple Service Discovery Protocol [9].

Por sua vez, o CharGEN *Flooding* procura explorar o funcionamento do protocol CharGEN, mais especificamente, o seu procedimento de responder a pedidos *Transmission Control Protocol* (TCP) ou UDP via porta 19 com, respetivamente, caracteres arbitrariamente gerados e números aleatórios. Assim, um atacante pode efetuar o *spoofing* do endereço IP do seu alvo, enviando, posteriormente, uma quantidade substancial de pedidos TCP ou UDP a dispositivos que empregam o protocolo CharGEN, nomeadamente impressoras e fotocopiadores que, ao responderem aos a estes pedidos da forma supramencionada, vão promover uma quantidade considerável de tráfego na porta 19 do sistema alvo. Deste modo, no caso concreto da *firewall* do sistema alvo não bloquear esta mesma porta, o servidor pode ficar sobrecarregado com o processo de análise e posterior resposta a todos os pedidos que recebeu [9], [10].

O protocol ICMP consiste na comunicação entre dispositivos de rede, mediante o envio de mensagens de erro específicas e de comandos de informação operacional, nomeadamente *Timestamp*, *Time Exceeded error*, *Echo Request* e *Echo Reply*. Assim, importa notar que estas 2 últimas mensagens podem ser empregues de forma conjunta, de modo a constituir o comando *ping*. Deste modo, cabe realçar a possibilidade de caracterizar o ICMP *Flooding* de 2 formas distintas, a saber: *Ping Flooding* e *Fragmentation Flooding*. No primeiro caso, os atacantes utilizam uma quantidade substancial de dispositivos para enviar pacotes *spoofed* ICMP *Ping* a diversos servidores. Assim, estes servidores, de modo a cumprirem os requisitos estabelecidos no protocolo ICMP, necessitam de responder aos pedidos, mediante o envio de um pacote resposta para o sistema alvo, já que os pacotes ICMP *Ping* possuem o endereço IP deste mesmo como emissor, promovendo uma sobrecarga deste mesmo, dado que irá receber num curto espaço temporal uma quantidade enorme de pacotes. Por sua vez, no segundo caso, os atacantes visam substituir cada pacote ICMP com o seu respetivo comando por diversos pacotes, de modo a fragmentar este mesmo. Assim, o sistema alvo, ao receber estes pacotes, vai proceder à sua reconstrução, de modo a obter o comando no seu estado original e, consequentemente, vai exaustar recursos ao tentar estabelecer conexões entre fragmentos intencionalmente não relacionados [9].

No caso concreto dos ataques que procuram explorar aplicações indevidamente utilizadas, importa realçar que, os atacantes, visam comprometer aplicações de alto tráfego em servidores legítimos, nomeadamente servidores *peer-to-peer*, de modo a que o tráfego destas seja redirecionado para um sistema alvo, permitindo, assim, que o atacante saia do sistema e que este funcione autónomamente. Nesta senda, importa realçar que as aplicações comprometidas vão procurar estabelecer conexões válidas com o sistema alvo, promovendo a sobrecargar deste. Mais se acrescenta que, a grande parte das ferramentas de proteção frequentemente utilizadas vão permitir estas tentativas de conexão, já que os pacotes enviados pelas aplicações comprometidas vão ser corretamente formatados e compostos [9].

Importa, ainda, notar que no ano de 2020 o serviço *Amazon Web Services* foi alvo de um *Volumetric DDoS Attack* de 2.3 *Terabits* por segundo de largura de banda, representado este um dos mais recentes e impactantes ataques da sua categoria. Neste seguimento, o ataque em questão foi concretizado via

exploração do protocolo *Connection-less Lightweight Directory Access Protocol*, de modo a inundar serviço em questão com um volume significativo de tráfego irrelevante. Mais se acrescenta que foram necessários diversos dias para que a equipa encarregue de solucionar este constragimento fosse capaz de mitigar por completo o ataque [10], [11].

2) Protocol Attacks

TODO

3) Protocol Attacks

TODO

C. Mecanismos de Deteção

TODO

D. Ferramentas e plataformas utilizadas

TODO

E. Motivações e Impactos

TODO

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/

[7] "What is a Botnet? Kaspersky," Sep. 2017, section: Threats. [Online]. Available: https://www.kaspersky.com/resource-center/threats/botnet-attacks

[8] "What is a Botnet?" [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-botnet

[9] C. Kime, "Complete Guide to the Types of DDoS Attacks," Dec. 2022. [Online]. Available: https://www.esecurityplanet.com/networks/types-of-ddos-attacks/

[10] "Different Types of DDoS Attacks Explained | ConnectWise," Aug. 2023. [Online]. Available: https://www.connectwise.com/blog/cybersecurity/types-of-ddos-attacks

[11] P. Nicholson, "AWS hit by Largest Reported DDoS Attack of 2.3 Tbps," Jun. 2020. [Online]. Available: https://www.a10networks.com/blog/aws-hit-by-largest-reported-ddos-attack-of-2-3-tbps/

Ricardo Pereira Biography text here.

André Filho Biography text here.