Análise a Ataques *Distributed Denial-of-Service*

Ricardo Pereira, André Filho

***Resumo*—A evolução tecnológica apresenta uma progressiva e crescente interconetividade, entre dispositivos eletrónicos que, consequentemente, define os ataques *Distributed Denial-of-Service* (DDoS), que visam comprometer a disponibilidade de diversas categorias de sistemas, como uma das ameaças mais significativas ao panorama global da cibersegurança. Deste modo, a clarificação do âmbito dos ataques DDoS revela-se indubitável na constituição de uma proteção considerável contra estes. Assim, o presente documento atingiu o seu objetivo, mediante o facultamento de informação suficiente e relevante no âmbito dos ataques DDoS, de modo a proporcionar uma perspetiva abrangente e detalhada sobre esta temática. Nesta senda, cabe notar que são abordados diversos conceitos sobre os ataques DDoS, categorias, ferramentas utilizadas na sua execução, assim como impactos e motivações destes. Neste seguimento, foi, também, realizada uma demonstração prática no âmbito do comportamento de uma *robot network*, que permitiu tirar ilações relevantes sobre o funcionamento destas redes, assim como a importância da escalabilidade nestas. Mais se acrescenta que foram analisadas diversas complicações e estratégias associadas ao processo de mitigação de ataques DDoS, assim como efetuada uma reflexão sobre o futuro desta temática.**

***Palavras-chave*—ataques, cibersegurança, *Distributed Denial-of-Service*, interconetividade, mitigação, *robot network*.**

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].

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. Nesta senda, cabe notar o ataque de DDoS realizado à Microsoft, mais especificamente, ao serviço Microsoft Azure, assim como alguns serviços Microsoft 365, que resultou numa indisponibilidade deste pelo período temporal de 8 horas. Mais se acrescenta que, em agosto de 2024, foi realizado um ataque DDoS que alcançou 7.5 mil milhões de pedidos por segundo ao banco ucraniano Monobank, mediante exploração da dependência deste na sua plataforma *mobile*, almejando paralisar as suas operações e destruir a confiança dos seus clientes [5].

Este documento visa clarificar 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 sua capacidade disruptiva.

Cumpre, ainda, esclarecer a estrutura do presente documento. Este relatório encontra-se organizado em 6 capítulos.

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

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 conclusão concisa 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 inteligência [6], [7].

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 potência 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 domínio 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 [6], [7].

Neste seguimento, o atacante, via o dispositivo *bot herder*, emprega a estratégia de *Command-and-control* (C2) 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 hierarquicamente, 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* [6].

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, monitoramento das atividades do utilizador, procura por vulnerabilidades e a instalação e execução de qualquer aplicação. Assim, a construção de uma BOTNET pode ser organizada em 3 fases distintas, a saber [6]:

- Preparação e Exposição: o atacante, inicialmente, procura por uma vulnerabilidade num dos tipos de dispositivos supramencionados, visando descobrir uma falha que possibilite uma infeção sem rastro deste mesmo dispositivo.
- 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*.
- 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*.

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 [6].

B. Categorias de ataques DDoS

A categorização das distinções entre ataques DDoS permite aprimorar a compreensão que indivíduo possuí destes. Nesta senda, cabe notar que existem 3 categorias principais de ataques de DDoS, a saber: *Volumetric DDoS Attacks*; *Protocol Attacks*; *Application Attacks* [8], [9].

As 3 categorias supramencionados facilitam a caracterização da grande parte de ataques DDoS. Contudo, 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 consideravelmente mais complicados de detetar e mitigar [8], [9].

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 [8].

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 [8]. 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 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 [8].

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 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 [8], [9].

O protocolo 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 [8].

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 que o tráfego destas seja redirecionado para um sistema alvo, permitindo, assim, que o atacante saia do sistema e que este funcione autonomamente. Nesta senda, importa realçar que as aplicações comprometidas vão procurar estabelecer conexões válidas com o sistema alvo, promovendo a sobrecarga 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 [8].

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 constrangimento fosse capaz de mitigar por completo o ataque [9], [10].

2) Protocol DDoS Attacks

Os *Protocol Attacks* procuram explorar protocolos, de modo a sobrecarregar um recurso público específico, nomeadamente servidores, mas, também, *firewalls* ou *load balancers* constrastando, assim, como os *Volumetric DDoS Attacks*, dado que não é utilizada uma quantidade substancial de uma matéria, principalmente *requests*, para concretizar o ataque de negação de serviço distribuída, mas sim apenas uma falha. Mais se acrescenta que a magnitude dos *Protocol Attacks* é medida mediante cálculo dos pacotes por segundo que este envia [8].

Neste seguimento, cabe notar os ataques IP *Null* onde os atacantes procuram definir o *header* de um pacote IPv4 como nulo e sem instruções específicas no âmbito da descarta do pacote, de modo a promover que o servidor destinatário deste consuma recursos substanciais numa tentativa fútil de determinar como proceder com o processo de comunicação, mais especificamente a entrega do pacote [8].

Importa, também, realçar os ataques de TCP *Flooding* que procuram explorar diretamente as características do protocolo TCP. Assim, estes ataques visam exaustar os recursos do sistema alvo, utilizando a estrutura do próprio protocolo, assim como via utilização de técnicas de *spoofing* e pacotes mal formados. Nesta senda, cabe notar que estas práticas permitem, a um atacante, constituir uma disrupção substancial no âmbito da disponibilidade do seu alvo, sendo, consequentemente, relevante realçar as diversas categorias distintas de ataques de TCP *Flooding* existentes, a saber: SYN *Flooding*; SYN-ACK *Flooding*; ACK *Flooding*; ACK *Fragmentation Flooding*; RST/FIN *Flooding*; *Multiple* ACK *Spoofed Session Flood*; *Multiple* SYN-ACK *Spoofed Session Flood*; *Synonymous* IP *Attack* [8], [9].

Além dos ataques que procuram explorar diretamente o protocolo TCP, importa notar outras abordagens que empregam diversos protocolo e técnicas, de modo a concretizar ataques de negação de serviço distribuídos. Neste seguimento, cabe notar que, estes ataques, utilizam, frequentemente, vulnerabilidades inerentes de protocolos habitualmente empregues por inúmeros serviços, aplicações e servidores na Internet. Além disso, são, também, executadas estratégias de *flooding*, de modo a aumentar a quantidade de tráfego enviado e, consequentemente, a cifra de recursos consumidos pelo sistema alvo. Mais se acrescenta que estes ataques, apesar de possuírem diversas implementações distintas, partilham o mesmo intuito de comprometer a disponibilidade do seu alvo, assim como possuem a capacidade de serem empregues em conjunto com outros vetores de ataque, promovendo uma dificuldade considerável no âmbito da sua mitigação. Deste modo, cumpre realçar as diversas categorias de ataques abrangidos pelas características supramencionadas, a saber: *Session Attacks*; Slowloris; *Ping of Death*; *Smurf Attack*; *Fraggle Attack*; *Low Orbit Ion Cannon*; *High Orbit Ion Cannon* [8], [9].

3) Application DDoS Attacks

No âmbito dos DDoS *Application Attacks* importa realçar que estes procuram explorar vulnerabilidades em aplicações, de modo a causar falhas na própria aplicação. Deste modo, cabe notar que, ao contrário de outras categorias de ataques DDoS, mais especificamente aqueles que visam comprometer a disponibilidade de um dispositivo ou infraestrutura, os ataques de aplicações concentram-se em comprometer a camada 7 do modelo *Open Systems Interconnection* (OSI). Contudo, estes ataques podem, também, resultar em processadores sobrecarregados, assim como memórias exaustas, afetando, inclusivamente, o servidor e outras aplicações. Assim, releva realçar que a magnitude de um *Application Attack* é medida em pedidos por segundo. Mais se acrescenta que os principais ataques DDoS de aplicações incluem *Hypertext Transfer Protocol* (HTTP) *Flood Attacks* e ReDoS [8], [9].

Nesta senda, cabe notar que os ataques de HTTP *Flood* procuram explorar os comandos HTTP, de modo a sobrecarregar *websites*, os servidores que hospedam estes, assim como a largura de banda emprega para os alcançar, mediante utilização de uma BOTNET. Assim, os *bots* utilizados nestes ataques permitem o envio de múltiplos pedidos sequencialmente, de modo que cada *bot* constituinte da rede permita aumentar exponencialmente o tráfego enviado para o *website* alvo. Deste modo, importa realçar os diversos tipos de ataques de HTTP *Flood* existentes, a saber [8]:

- Ataques de GET: o atacante procura enviar um volume substancial de pedidos concorrentes GET de ficheiros de dimensão considerável, nomeadamente vídeos e ficheiros *Portable Document Format* (PDF).
- Ataques de POST: o atacante visa enviar um volume considerável de pedidos concorrentes POST de ficheiros de dimensão notável, nomeadamente vídeos e ficheiros PDF.
- *Long-and-Slow* POST *Attacks*: o atacante procura enviar pedidos HTTP POST que indicam o envio de enormes quantidades de dados de uma só vez, mas, na realidade, este envia quantidades mínimas de dados, de forma espaçada. Mais se acrescenta que estes ataques frequentemente empregam a ferramenta R-U-Dead-Yet que possibilita o envio de dados nos moldes necessários a este tipo de ataque [11].
- *Single Session or Request Attack*: o atacante visa explorar uma vulnerabilidade presente na versão 1.1 do protocolo HTTP, mais especificamente a possibilidade de enviar múltiplos pedidos distintos no *header* de um único pacote.
- *Fragmented* HTTP *Flood*: o atacante procura que os *zombies* da sua BOTNET estabeleçam conexões HTTP válidas com sistema alvo enviando, posteriormente, pacotes fragmentados de baixa dimensão a uma velocidade curial aos mínimos aceites pelo servidor neste horizonte. Assim, é possível evadir diversas defesas contra ataques DDoS, já que, dadas as características do ataque, a atividade aparenta ser legítima. Deste modo, o servidor mantém a sessão ativa e, consequentemente, consome recursos com largura de banda reservada. Mais se acrescenta que este tipo de ataque pode ser concretizado via utilização da ferramenta Slowloris.
- *Recursive* GET *Flooding*: o atacante visa sobrecarregar o servidor alvo, mediante o envido de pedidos GET no âmbito da obtenção de longas listas de páginas ou imagens. Assim, este ataque possibilita o consumo de

recursos enquanto aparenta ser atividade legítima.
- *Random Recursive* GET *Flooding*: o atacante executa um ataque, essencialmente, análogo ao *Recursive* GET *Flooding*, mas emprega uma abordagem que permite selecionar aleatoriamente as páginas requisitadas nos pedidos enviados.

No caso concreto do ataque ReDoS, cabe notar que este emprega *regular expressions*, de modo a concretizar um ataque de DDoS. Assim, o atacante constitui pedidos que visam obter quantidades extraordinariamente elevadas e complexas de padrões de pesquisa, possibilitando a exaustão de recursos ou, potencialmente, o acontecimento de *crashes* no sistema alvo [8].

C. Ferramentas utilizadas

Existem inúmeras ferramentas que possibilitam a concretização de um ataque DDoS, nomeadamente os *stressors*. Neste seguimento, cabe notar que, esta categoria, é constituída por um conjunto extenso de outras ferramentas construídas, de modo a possibilitar a realização de um *stress test* a uma rede. Assim, dadas esta capacidade intrínseca de sobrecarregar uma rede, estas ferramentas podem, também, ser empregues em ataques de DDoS. Mais se acrescenta que, estas ferramentas, possuem níveis de especialidade distintos, já que, algumas, são capazes de executar ataques mediante múltiplos vetores distintos, enquanto outras especializam-se em concretizar ofensivas numa determinada camada do modelo OSI [12], [13].

Nesta senda, cumpre clarificar algumas categorias de ferramentas empregues em ataques de DDoS, a saber: *Long and slow attack tools*; *Application Layer attack tools*; *Protocol Layer attack tools* [12].

No caso concreto das primeiras ferramentas, tal como o nome indíca, estas proporcionam a possibilidade de realizar ataques DDoS *Long and Slow*, já que a metodologia consite em enviar para o seu alvo uma quantidade baixa de volume de dados a uma velocidade muito lenta. Deste modo, estas ferramentas permitem efetuar a manutenção de conexões, em múltiplas portas, com um sistema alvo durante longos períodos, promovendo um consumo considerável de recursos deste mesmo. Mais se acrescenta que, estas ferramentas, podem, inclusivamente, ser eficientes na concretização de um ataque DDoS, sem a necessidade de utilizar uma BOTNET, sendo frequentemente empregues por atacantes que só possuem acesso a um único dispositivo [12], [13].

Por sua vez, as segundas, executar ataques DDoS de aplicações, mais especificamente ofensivas deste tipo que procuram comprometer a camada 7 do modelo OSI. Assim, um atacante, mediante utilização destas ferramentas e, consequentemente, de uma das técnicas explanada no ponto II.B.3, pode lançar uma quantidade desproporcionada de pedidos a um sistema alvo. Mais se acrescenta que, este tráfego adicional, revela dificuldade de deteção, ou seja, é complicado para as defesas do alvo distinguirem este de pedidos normais, efetuados por utilizados legítimos [12].

As terceiras ferramentas supramencionadas, procuram explorar vulnerabilidades presentes em protocolos, de modo a comprometer a disponibilidade de um sistema alvo. Deste modo, importa realçar que, estas ferramentas, são, habitualmente, empregues por BOTNETs, já que a magnitude do ataque promovido por estas aumenta, consideravelmente, com o acréscimo de quantidade de dispositivos que pertencem a este. Mais se acrescenta que, quando empregues num único dispositivo, estes utensílios podem ser totalmente ineficientes [12].

D. Impactos e Motivações

Cada ataque DDoS possuí características que o distinguem dos demais, inclusivamente no que aos impactos e motivações diz respeito.

No âmbito dos impactos, cabe notar o prejuízo financeiro associado a um ataque DDoS bem-sucedido a uma organização, já que estes podem causar um decréscimo de produtividade dos funcionários desta mesma, indisponibilidade dos seus serviços, inclusivamente, podendo agravar esta consequência mediante a potencial perda de clientes e perda global de rendimentos, via incapacidade de realizar os seus processos de negócio. Além disso, vão, também, existir custos associados à recuperação dos sistemas afetados, assim como à implementação de medidas que possibilitem precaver e mitigar futuros ataques. Mais se acrescenta que, estes ataques, podem, também, causar complicações legais, mais especificamente disputas entre a organização que sofreu o ataque e os seus clientes, potencialmente agravando, assim, os prejuízos financeiro associado ao ataque [9], [14], [15].

Nesta senda, importa, também, realçar que os ataques DDoS podem ser particularmente prejudiciais para a reputação de uma organização, nomeadamente para empresas que proporcionam serviços onde a disponibilidade revela-se imperativa. Assim, no caso concreto destas empresas, um ataque à disponibilidade dos seus serviços, devido ao *downtime* que causa, pode danificar gravemente a reputação desta mesma, assim como a sua relação com clientes e parceiros. Mais se acrescenta que, um ataque DDoS pode, inclusivamente, revelar vulnerabilidades e fraquezas adicionais nos sistemas de uma organização, assim como na sua rede interna que facultam a possibilidade de, posteriormente, serem executados outros tipos de ataques que exploram estes mesmos [9], [14], [15].

Por sua vez, no âmbito das motivações, cabe notar que os atacantes justificam as suas ações com base em ganhos financeiros, via utilização de diversas técnicas, nomeadamente extorsão e *blackmailing*, onde são efetuadas promessas de interromper os ataques, mediante o pagamento de um valor de resgate. Além disso, os ataques podem ser perpetrados por um indivíduo que possua a necessidade de vingança para com uma organização específica ou outro indivíduo, assim como por alguém que procura comprovar as suas capacidades ou que apenas possuí o intuito de obter satisfação pessoal [14], [16].

Neste seguimento, importa, também, realçar que os ataques DDoS podem ser motivados por ações de *hackvism*, onde um atacante procura utilizar estes ataques para chamar atenção e protestar um político, política ou ideologia, assim como governos e outras instituições relevantes, nomeadamente ad-

ministrativas ou políticas. Mais se acrescenta que a *cyber-warfare* demonstra ser um assunto progressivamente mais perentório, no horizonte de ataques DDoS, já que estes são crescentemente utilizados por países, de modo a possibilitar o comprometimento de diversos aspetos de outros países, permitindo, assim, obter ganhos políticos e militares [14], [16].

III. Demonstração Prática

De modo a exemplificar os conceitos enunciados no capítulo II, foi realizada uma demonstração prática que almejou, fundamentalmente, constituir uma BOTNET de pequena dimensão, num ambiente controla. Assim, foram desenvolvidas diversas ferramentas, com o apoio de bibliotecas *open source*, que possibilitaram o estabelecimento de um fluxo automático de informação entre um operador humano e um alvo digital.

Neste seguimento, o ambiente em questão, foi implementado localmente, mediante utilização de uma rede local, assim como 3 computadores. Mais se acrescenta que 2 dos computadores desempenharam o papel de *bot*, enquanto que o restante dispositivo desempenhou o papel de servidor C2 e sistema alvo.

A. Processo de Setup

Para a implementação do ambiente, foi utilizada a linguagem de programação Python, mais especificamente a versão 3.12 desta mesma, já que as versões posteriores apresentam diversos problemas de compatibilidade com as bibliotecas empregues.

Deste modo, cumpre esclarecer as ferramentas utilizadas pelos intervenientes da demonstração prática, a saber:

- *Bots*: funcionalidades de DoS disponibilizadas pelo projeto Bane [17]. Nesta senda, cabe notar que foram utilizados o módulo relacionado com um ataque DDoS. De modo a instalar este, foi necessário utilizar a supramencionada versão do Python, assim como efetuar a importação deste. Mais se acrescenta que os *bots* possuem um servidor cliente próprio, cujo possibilita a comunicação com o controlador C2 e, consequentemente, a obtenção de comandos e o envio de relatórios para este, procurando clarificar o estado das operações.
- Servidor C2: qualquer servidor capaz de receber pedidos HTTP será suficiente. Assim, foi empregue a ferramenta Flask, que se revelou curial às necessidades da demonstração.
- Servidor Alvo: foi constituído um servidor simples que somente regista os pedidos que recebe. Mais se acrescenta que foi utilizado o módulo Beszel [18], de modo a monitorizar o tráfego recebido, já que este possuí requisitos mínimos de implementação.
- Operador: procura comunicar com o servidor C2, via pedidos HTTP. De modo a possibilitar isto mesmo, foi disponibilizada, em formato de texto, a totalidade de comandos *Invoke-WebRequest* possíveis no ficheiro ”c2_server_commands”.

B. Arquitetura e Execução

No âmbito da arquitetura de sistema implementa, cabe notar que esta se encontra dividida em 4 setores, a saber: operador; servidor C2; *bots*; servidor alvo. Neste seguimento, a Figura 1 apresenta o fluxo de informação desta mesma arquitetura.

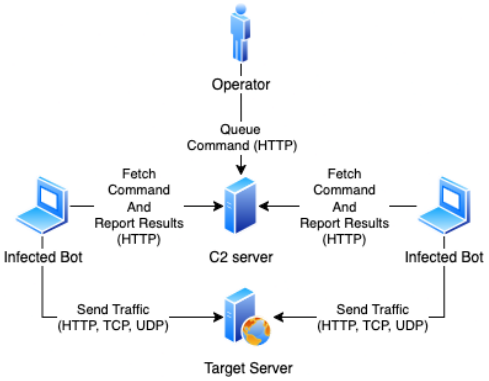

Fig. 1. Arquitetura do ambiente de teste

Assim, é possível observar que o processo inicia no operador, que envia um pedido HTTP ao servidor C2. Este pedido contém a instrução sobre o tipo de ataque a ser executado pelos *bots*. Neste seguimento, importa realçar que o servidor C2 encontra-se preparado para escutar pedidos provenientes do operador, mas também dos *bots*. Assim, aquando da receção de um pedido, o servidor C2 armazena este numa fila até ao seu processamento ou coleta pelo mecanismo *garbage collector*. Mais se acrescenta que as instruções de ataque somente podem ser interpretadas pelos *bots* 1 vez, garantindo a unicidade da execução.

Nesta senda, paralelamente ao processo suprarreferido, os *bots* efetuam requisições ao servidor C2 de forma cíclica, verificando, inclusivamente, a existência de novos ataques na fila. Assim, quando um pedido é identificado, o servidor proporciona as instruções necessárias para que cada *bot* compile os resultados do *stdout* e do *stderr* do procedimento de ataque, limitando esta captura aos últimos 300 caracteres. Este limite, via uma análise efetuada, demonstrou ser suficiente para determinar a correta execução do ataque, assim como obter informações relevantes sobre o processo.

Posteriormente, o *bot* retorna ao estado de monitorização, verificando se há novos comandos disponíveis na fila, repetindo-se assim o ciclo. Cumpre, ainda, salientar que os *bots* possuem a capacidade de executar 5 tipos distintos de ataques, conforme as instruções recebidas do servidor C2, a saber: HTTP_PUNCH; HTTP_SPAM; TCP_FLOOD; UDP_FLOOD e SLOW_READ. Mais se acrescenta que estes ataque permitem assegurar a diversidade e a flexibilidade nas estratégias ofensivas.

C. Resultados obtidos

Após a conclusão da constituição do ambiente, foram realizadas diversas rondas de testes para cada um dos ataques supramencionados, cujos dados podem ser consultados nas Tabelas I, II e III. Neste seguimento, cabe notar que todos os ataques foram realizadas via servidor C2, possuindo uma

duração máxima de 30 segundos. Mais se acrescenta que os computadores empregues estavam equipados com o sistema operativo Windows 11 e somente possuíam a aplicação de linha de comandos em execução durante os testes.

Tabela I
ANÁLISE DE MÉTRICAS EM ESTADO *idle*

	Idle
NET	7Kb
CPU	1.5%

Tabela II
ANÁLISE DE MÉTRICAS COM A UTILIZAÇÃO DE 1 *bot*

	H_P	H_S	T_F	U_F	S_R
NET	6MB	7MB	1.3MB	170Kb	20Kb
CPU	4%	7.5%	6%	8%	3%

Tabela III
ANÁLISE DE MÉTRICAS COM A UTILIZAÇÃO DE 2 *bots*

	H_P	H_S	T_F	U_F	S_R
NET	8MB	9MB	2MB	200Kb	30Kb
CPU	5%	8%	7%	13%	3%

Mediante análise às informações suprarreferidas, é possível compreender que estas proporcionam uma perspetiva abrangente das condições experimentais do ambiente, assim como dos resultados obtidos. Deste modo, é possível tirar ilações sobre a potencial magnitude de um atacante utilizando uma BOTNET, mais especificamente quanto maior a cifra de dispositivo maior será o impacto do ataque. Mais se acrescenta que, embora não tenham ocorrido repercussões significativas, o sistema de testes, ao ser submetido a uma BOTNET maior, seria capaz de ser derrubado.

IV. DESAFIOS E ESTRATÉGIAS NA MITIGAÇÃO

A prevenção de ataques DDoS revela ser um processo de dificuldade significativa, dada a existência de múltiplos fatores que condicionam este processo. Neste seguimento, cabe notar a natureza distribuídas destes ataques complica este processo, dado que são, habitualmente, empregues BOTNETs constituídas por uma cifra imensa de dispositivos distintos, que não possibilitam um bloqueamento de tráfego eficiente, já que existe uma imensurável quantidade de fontes deste mesmo. Deste modo, importa, também, realçar o volume de tráfego associado a um ataque DDoS que, em ataques modernos, pode facilmente sobrecarregar a largura de banda de uma rede. Além disso, a variedade de ataques DDoS existente possuí a consequência de promover uma necessidade de adorar estratégias defensivas em camadas, mediante diversas técnicas, nomeadamente *web application firewalls*, *rate limiting*, DNS-*Based traffic management*. Mais se acrescenta que os ataques DDoS tem apresentado um crescimento notório na sua sofisticação, mediante utilização de técnicas avançadas que permitem evadir processos de deteção e maximizar os impactos, assim como a utilização de múltiplos vetores de ataque consecutivamente e a crescente acessibilidade a serviços de *DDoS-as-a-Service* que possibilitam, a utilizadores isentos de conhecimentos relevantes à execução de um ataque DDoS, realizar ataques, via realização, unicamente, de um pagamento [5], [16], [19].

No âmbito da deteção de ataques DDoS, importa realçar que este processo envolve, essencialmente, o reconhecimento de sinais que indicam que o sistema encontra-se como alvo de ataque. Assim, revela-se imperativo notar estes mesmos sinais, a saber [14]:

- Aumento súbito e inesperado de tráfego de rede de uma localização específica ou de um endereço IP particular
- Desempenho fraco e irregular da rede, nomeadamente no âmbito dos tempos de carregamento dos *websites* e da disponibilidade global dos serviços. Mais se acrescenta que um abrandamento considerável de um sistema é um sinal evidente de que este se encontra sob um ataque DDoS.
- Mensagens de erro de servidores, *timeouts* e incapacidades em aceder a serviços e aplicações inexplicáveis. Assim, aquando destas circunstâncias, um atacante conseguiu comprometer a disponibilidade do sistema. Mais se acrescenta que, no caso concreto de um ataque DDoS de grau superior de seriedade, estas complicações não serão resolvidas mediante, exclusivamente, redução do tráfego de rede que chega a esta.
- Queixas, por parte dos funcionários, sobre uma conetividade de rede fraca. Mais se acrescenta que, este sinal, revela principal utilidade em circunstâncias onde a rede utilizada pelos funcionários é a mesma que a rede empregue pelos serviços, servidores e aplicações da organização.
- Desempenho transversalmente reduzido de dispositivos pertencente à mesma rede. Neste caso concreto, é possível perspetivar que o atacante comprometeu com sucesso a largura de banda da rede, minimizando a disponibilidade desta para os dispositivos que de si dependem.
- Notificações do *Internet Service Provider*,*Cloud Service Provider*, assim como outros fornecedores de serviços empregues.

Nesta senda, cabe, também, notar que existem métodos automatizados que permitem a deteção de ataques DDoS, nomeadamente ferramentas como *Intrusion Detection Systems* e *Security Information and Event Management*, que proporcionam um alerta célere e eficiente dos administradores, numa circunstância em que algum sistema, abrangido por estes, seja alvo de um ataque [20].

No caso concreto de proteção e mitigação, releva realçar que são adotadas diversas técnicas e estratégias, de modo a redirecionar, para um *scrubbing center* ou utilizando *load balancers*, o tráfego resultante de um ataque DDoS, de forma célere e eficiente. Além disso, as organizações, atualmente, adotam, também, diversas tecnologias que permitem identificar e intercetar tráfego malicioso, a saber [2]:

- *Web application firewalls*: quando utilizadas em conjunto com outras defesas periféricas, permitem proteger a rede, assim como as aplicações de atividade maliciosa, medi-

ante análise a cada pacote no tráfego de rede, de modo a identificar e bloquear tráfego malicioso.

- Content Delivery Networks: permitem agilizar o acesso dos utilizadores a recursos *online*, via a utilização de uma rede de servidor distribuídos, sendo que, no caso concreto em que esta é impactada por um ataque DDoS, é possível alterar o trajeto do tráfego legítimo para outros servidores que possuam recursos disponíveis.
- *Security Information and Event Management*: proporcionam diversas funções de deteção de ataques DDoS antecipadamente, mediante a análise de eventos de segurança, assim como a monitorização de tráfego de rede, alertando os administradores, aquando da deteção de atividade maliciosa.

Nesta senda, cabe, também, notar a existência de tecnologias de proteção e mitigação de ataques DDoS de última geração, a saber: *Cloud-based mitigation*; *AI-Driven traffic analysis*.

A primeira, proporciona proteções aos sistemas, via utilização de infraestruturas em nuvem, de modo a absorver, filtrar e mitigar tráfego malicioso, previamente à chegada deste ao sistema. Neste seguimento, esta tecnologia possuí no seu cerne 4 etapas distintas, de modo a combater o ataque, a saber: Deteção, procurando identificar tráfego malicioso; Resposta, visando abandonar tráfego malicioso; Encaminhamento, procurando proporcionar um redirecionamento eficiente de tráfego; Adaptação, visando ajustar as defesas do sistema [21].

Por sua vez, a segunda, possibilita a identificação de tráfego malicioso de forma célere e eficiente, via utilização de algoritmos de *Machine Learning* que analisam o tráfego de uma rede continuamente, de modo a identificar anomalias e a bloquear ameaças. Nesta senda, cabe notar que, a utilização destes algoritmos possibilita uma deteção de ameaças dinâmica, já que é possível alterar as regras de deteção em tempo real, permitindo ajustar estas a cada circunstância específica. Assim, esta adaptabilidade faculta proteções consideráveis no âmbito de ataques DDoS que empregam múltiplos vetores de ataque. Mais se acrescenta que o processamento, por parte dos algoritmos, de um volume progressivamente crescente de dados, permite que estes efetuem um aprimoramento significativo das suas capacidades, sendo que estas novas aptidões revelam-se cruciais na manutenção do desempenho e disponibilidade dos sistemas, em circunstâncias onde são requisitadas respostas imediatas e precisas [22].

V. Perspetiva futura

Os ataques de DDoS, atualmente, representam uma ameaça formidável ao panorama global da cibersegurança. Nesta senda, cabe notar que, o avanço da tecnologia proporciona novas possibilidades de atacantes constituírem novos ataques DDoS que empregam novos métodos, estratégias e vetores de ataque, procurando construir uma ofensiva progressivamente mais destrutiva. Assim, as organizações, de modo a garantir a proteção dos seus sistemas, devem possuir uma constante atenção ao mundo digital, mais especificamente aos avanços tecnológicos que possam ser utilizados para a constituição e concretização de novos ataques DDoS.

No âmbito de tendências emergentes relevantes ao contexto, importa realçar o crescimento de complexidade dos ataques DDoS, mais especificamente a utilização de múltiplos vetores de ataque. Deste modo, os ataques DDoS do futuro serão, possivelmente, muito mais sofisticados que os atuais e, consequentemente, muito mais destrutivos e difícil de mitigar. Além disso, o crescimento da quantidade de dispositivos IoT constituí uma ameaça substancial, já que estes possuem o potencial de aumentarem, significativamente, a quantidade de *bots* em cada BOTNET, principalmente, pois estes possuem uma ausência de defesas robustas que, consequentemente, facilitam a sua infeção por parte de um atacante. O crescimento da inteligência artificial, assim como dos algoritmos de *machine learning* permitem a constituição de novas defesas contra ataques DDoS, explanado no capítulo 4. Contudo, este aumento de preponderância destas tecnologias permite, também, a constituição de novos esquemas de ataques, proporcionando ataques dinâmicos com um elevado grau de adaptabilidade e, consequentemente, imensamente complexos e sofisticados. Mais se acrescenta que é possível perspetivar que os ataques DDoS possam ser, futuramente, utilizados como uma ferramenta de distração, de modo a viabilizar ataques informáticos mais sofisticados e complexos, que visam obter ilicitamente informações sensíveis e causar disrupções a infraestruturas críticas [23].

VI. Conclusão

O presente documento proporciona uma análise detalhada dos ataques DDoS. Deste modo, parece adequado afirmar que o objetivo de proporcionar informação suficiente e relevante sobre a temática foi atingido. Assim, cabe notar que são abordados os mecanismos operacionais, efetuadas categorizações e evidenciadas as ameaças que estes ataques representam no atual panorama global da cibersegurança.

Importa realçar que, mediante investigação ao conceito de BOTNETs, mais especificamente às suas características e arquiteturas, foi possível demonstrar informação pertinente sobre a temática, já que estas redes de computadores infetados são, frequentemente, empregues em ataques DDoS. Neste seguimento, a demonstração prática efetuada permitiu simular, em ambiente controlado, um ataque DDoS de pequena escala, sendo possível compreender, didaticamente, o *modus operandi* destas mesmas redes, demonstrando, inclusivamente, a importância da escalabilidade nestas.

Cabe, ainda, notar que foram analisadas diversas complicações e estratégias presentes do processo de mitigação de um ataque DDoS, nomeadamente procedimentos de deteção, ferramentas defensivas, *Cloud-based mitigation* e *AI-Driven traffic analysis*. Mais se acrescenta que a evolução da tecnologia, permite aprimorar a sofisticação destas medidas defensivas, mas também possibilita o aumento da acessibilidade a ferramentas que viabilizam a realização de ataques DDoS, assim como o crescimento de dispositivos IoT ausentes de defesas robustas que podem, facilmente, constituir BOTNETs.

No âmbito de trabalho futuro importa salientar a necessidade de efetuar abordagens à temática que possibilitem o

aperfeiçoamento do conhecimento sobre ataques DDoS que empregam múltiplos vetores de ataque, assim como ofensivas que utilizem inteligência artificial para aprimorar a sua capacidade destrutiva e dificultar a sua deteção.

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

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

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

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

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

[10] 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/

[11] "What is R.U.D.Y. (R-U-Dead-Yet?) | DDoS Tools | Imperva." [Online]. Available: https://www.imperva.com/learn/ddos/rudy-r-u-dead-yet/

[12] "How to DDoS | DoS and DDoS attack tools." [Online]. Available: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/how-to-ddos/

[13] "How to DDoS | Common DDoS Attack Tools | Radware." [Online]. Available: https://www.radware.com/cyberpedia/ddos-attacks/how-to-ddos-seven-common-ddos-attack-tools/

[14] C. S. E. Canada, "Defending against distributed denial of service (DDoS) attacks – ITSM.80.110," Jan. 2024, last Modified: 2024-02-23. [Online]. Available: https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110

[15] "Impact of DDoS Attacks on Businesses | StormWall," Aug. 2024. [Online]. Available: https://stormwall.network/resources/blog/impact-of-ddos-attacks-on-businesses

[16] Z. Brodsky, "The Psychology Behind DDoS: Motivations and Methods," Feb. 2020. [Online]. Available: https://www.perimeter81.com/blog/network/the-psychology-behind-ddos-attacks

[17] A. Bouali, "AlaBouali/bane," Jan. 2025, original-date: 2019-03-10T20:23:44Z. [Online]. Available: https://github.com/AlaBouali/bane

[18] hank, "henrygd/beszel," Jan. 2025, original-date: 2024-07-07T21:36:28Z. [Online]. Available: https://github.com/henrygd/beszel

[19] "DDoS Attack Prevention: Why It's Hard & 12 Ways to Prevent DDoS | Radware." [Online]. Available: https://www.radware.com/cyberpedia/ddos-protection/how-to-prevent-ddos-attacks-best-practices-strategies/

[20] S. Global, "The Rise of DDoS Attacks: Strategies, Challenges, and Best Practice." [Online]. Available: https://www.suntera.com/our-expert-commentary/the-rise-of-ddos-attacks

[21] "What is DDoS mitigation?" [Online]. Available: https://www.cloudflare.com/learning/ddos/ddos-mitigation/

[22] "What Are the Emerging Trends in AI-Driven Traffic Filtering for Enhanced DDoS Protection - Kaiyue January 10, 2025 Accelerate, Secure & Compute Your Global Business Streaming Content Data File Downloads Take your edge, to the next level," Nov. 2024. [Online]. Available: https://www.edgenext.com/what-are-the-emerging-trends-in-ai-driven-traffic-filtering-for-enhanced-ddos-protection/

[23] M. C. Ltd, "The Future of DDoS Security: Navigating Evolving Techniques with Adaptive Defence Strategies | Microminder Cybersecurity | Holistic Cybersecurity Services." [Online]. Available: https://www.micromindercs.com/blog/the-future-of-ddos-security-navigating-evolving-techniques

Ricardo Pereira (M, 23) é um estudante de Mestrado em Cibersegurança e Informática Forense no Instituto Politécnico de Leiria. Em 2024, licenciou-se em Engenharia Informática pela mesma instituição, onde desenvolveu diversas competências na área de informática, nomeadamente programação, desenvolvimento *web*, administração de bases de dados e inteligência artificial.

André Filho (M, 21) é um engenheiro de *software* na Interlog Group, onde concentrou a sua experiência profissional no desenvolvimento *web*. Licenciou-se em 2024 em Engenharia Informática pelo Instituto Politécnico de Leiria. Atualmente, frequenta o Mestrado em Cibersegurança e Informática Forense na mesma instituição, aprofundando os seus conhecimentos nesta área em crescimento.

Vídeo da demonstração da componente prática: https://www.youtube.com/watch?v=nWVITOYAwYE.

Código-fonte da demonstração prática, localizado na diretoria assi-demo: https://github.com/ricardomlpereira/assi-project.