

**MINISTÉRIO DA DEFESA  
EXÉRCITO BRASILEIRO  
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA  
INSTITUTO MILITAR DE ENGENHARIA  
CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO**

**1 Ten ROBERTO TADEU ABRANTES DE ARAÚJO  
TARIK BAUER VENTURA**

**PAINEL DE APOIO PARA UMA CENTRAL DE DETECÇÃO DE  
PADRÕES MALICIOSOS**

**Rio de Janeiro  
2019**

**INSTITUTO MILITAR DE ENGENHARIA**

**1 Ten ROBERTO TADEU ABRANTES DE ARAÚJO  
TARIK BAUER VENTURA**

**PAINEL DE APOIO PARA UMA CENTRAL DE DETECÇÃO  
DE PADRÕES MALICIOSOS**

Projeto de Fim de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Engenheiro de Computação.

Orientador: Prof. Sérgio dos Santos Cardoso Silva - M.Sc.  
Co-Orientador: Prof. Ronaldo Ribeiro Goldschmidt - D.Sc.

Rio de Janeiro  
2019

c2019

INSTITUTO MILITAR DE ENGENHARIA  
Praça General Tibúrcio, 80 - Praia Vermelha  
Rio de Janeiro - RJ CEP 22290-270

Este exemplar é de propriedade do Instituto Militar de Engenharia, que poderá incluí-lo em base de dados, armazenar em computador, microfilmear ou adotar qualquer forma de arquivamento.

É permitida a menção, reprodução parcial ou integral e a transmissão entre bibliotecas deste trabalho, sem modificação de seu texto, em qualquer meio que esteja ou venha a ser fixado, para pesquisa acadêmica, comentários e citações, desde que sem finalidade comercial e que seja feita a referência bibliográfica completa.

Os conceitos expressos neste trabalho são de responsabilidade do(s) autor(es) e do(s) orientador(es).

de Araújo, Roberto Tadeu Abrantes  
Painel de apoio para uma central de detecção de padrões maliciosos / Roberto Tadeu Abrantes de Araújo, Tarik Bauer Ventura, orientado por Sérgio dos Santos Cardoso Silva e Ronaldo Ribeiro Goldschmidt - Rio de Janeiro: Instituto Militar de Engenharia, 2019.

54p.: il.

Projeto de Fim de Curso (graduação) - Instituto Militar de Engenharia, Rio de Janeiro, 2019.

1. Curso de Graduação em Engenharia de Computação - projeto de fim de curso. 1. Segurança Cibernética. 2. Botnet. 3. Projeto EB-CyberDef. 4. Painel de Apoio. 5. Fluxos Maliciosos. 6. Oráculo. I. Silva, Sérgio dos Santos Cardoso. II. Goldschmidt, Ronaldo Ribeiro. III. Título. IV. Instituto Militar de Engenharia.

INSTITUTO MILITAR DE ENGENHARIA

1 Ten ROBERTO TADEU ABRANTES DE ARAÚJO  
TARIK BAUER VENTURA

PAINEL DE APOIO PARA UMA CENTRAL DE DETECÇÃO  
DE PADRÕES MALICIOSOS

Projeto de Fim de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Engenheiro de Computação.

Orientador: Prof. Sérgio dos Santos Cardoso Silva - M.Sc.

Co-Orientador: Prof. Ronaldo Ribeiro Goldschmidt - D.Sc.

Aprovado em 14 de Outubro de 2019 pela seguinte Banca Examinadora:



Prof. Sérgio dos Santos Cardoso Silva - M.Sc. do IME - Presidente



Prof. Ronaldo Ribeiro Goldschmidt - D.Sc. do IME



Prof. Julio Cesar Duarte - D.Sc. do IME



Prof. Leandro de Mattos Perreira - M.Sc. do IME

Rio de Janeiro  
2019

Ao Instituto Militar de Engenharia, alicerce da minha formação e aperfeiçoamento.

## AGRADECIMENTOS

Primeiramente, gostaríamos de agradecer a todas as pessoas que nos incentivaram e apoiaram no decorrer deste ano. Indubitavelmente, possibilitaram-nos cumprir com êxito nossa última missão neste nobre instituto.

Aos professores Sérgio Cardoso e Ronaldo Goldschmidt, que conseguiram nos fornecer todo o suporte necessário à realização do trabalho e guiar-nos para atingirmos o sucesso previsto.

Aos professores Leandro Ferreira e Julio Duarte, sempre precisos em cada avaliação, contribuindo para o constante progresso do projeto.

Por fim, ao Tio Almir, sempre presente em cada momento de dificuldade, proporcionando a ajuda necessária para superarmos com excelência cada desafio encontrado.

## SUMÁRIO

LISTA DE ILUSTRAÇÕES .....	8
<b>1 INTRODUÇÃO .....</b>	<b>11</b>
1.1 Motivação .....	12
1.2 Objetivo .....	12
1.3 Justificativa .....	13
1.4 Metodologia .....	14
1.5 Estrutura do Texto .....	14
<b>2 FUNDAMENTAÇÃO TEÓRICA .....</b>	<b>15</b>
2.1 Conceitos Importantes .....	15
2.2 Tipos de Ataque .....	17
2.2.1 Engenharia Social .....	17
2.2.2 Malware .....	18
2.2.3 (D)DoS .....	19
2.2.4 Botnet .....	20
2.2.4.1 Definição .....	20
2.2.4.2 Funcionamento .....	20
2.2.4.3 Componentes .....	22
2.2.4.4 Topologias de uma Botnet .....	23
2.3 Técnicas de Defesa .....	25
2.3.1 Monitoramento: da Estação x do Tráfego de Rede .....	25
2.3.2 Defesa: Passiva x Ativa .....	26
2.3.3 Detecção por: Assinatura x Comportamento .....	26
<b>3 EB-CYBERDEF .....</b>	<b>28</b>
3.1 Introdução ao Projeto .....	28
3.2 Estrutura do Projeto .....	28
<b>4 MÓDULO PAINEL DE APOIO .....</b>	<b>32</b>
4.1 Objetivo .....	32
4.2 Features Relevantes .....	32
4.2.1 Parecer do módulo de pré-processamento .....	32
4.2.2 Nome de Domínio .....	32

4.2.3	Data de registro do domínio .....	33
4.2.4	Geolocalização .....	33
4.2.5	Tipo do conteúdo de resposta .....	33
4.2.6	Top Level Domain .....	33
4.2.7	Presença do domínio em <i>blacklists</i> .....	33
4.2.8	Informações gerais acerca do Fluxo de Rede .....	34
4.2.9	Informações relativas à requisição HTTP .....	34
4.2.10	Registro do Domínio .....	34
4.3	Ferramentas .....	34
4.3.1	Linguagens de Programação .....	34
4.3.1.1	Python 3 .....	34
4.3.1.2	ECMAScript 6 .....	35
4.3.2	Web Frameworks .....	35
4.3.2.1	Sanic .....	35
4.3.2.2	React .....	35
4.3.3	Banco de Dados .....	36
4.3.3.1	MongoDB .....	36
4.4	Estrutura .....	37
4.4.1	EB-CyberDef-Server .....	38
4.4.1.1	run.py .....	38
4.4.1.2	requirements.txt .....	38
4.4.1.3	config.py .....	38
4.4.1.4	factory.py .....	38
4.4.1.5	logs .....	39
4.4.1.6	users .....	39
4.4.2	EB-CyberDef-Client .....	39
4.4.2.1	public/index.html .....	39
4.4.2.2	bundle.js .....	39
4.4.2.3	App.css .....	40
4.4.2.4	App.js .....	40
4.4.2.5	components .....	40
4.5	Protótipo .....	41
4.5.1	Interface Inicial .....	41
4.5.2	Interface de Registro dos Oráculos .....	42
4.5.3	Interface de Login .....	43



4.5.4	Listagem dos Tráfegos de Rede .....	43
4.5.5	Interface de Detalhamento do Tráfego de Rede .....	44
<b>5</b>	<b>CONCLUSÃO</b> .....	<b>46</b>
<b>6</b>	<b>REFERÊNCIAS BIBLIOGRÁFICAS</b> .....	<b>47</b>

## LISTA DE ILUSTRAÇÕES

FIG.2.1	Estrutura de uma típica Botnet. (KHATTAK et al., 2013) . . . . .	21
FIG.2.2	Topologia Hierárquica de uma Botnet. (UFRJ, 2015) . . . . .	24
FIG.2.3	Topologia Peer-to-Peer de uma Botnet. (CLOUDFLARE, 2018) . . . . .	25
FIG.3.1	Visão Macro-Funcional da Arquitetura da Fase de Produção/Operação do EB-CyberDef. . . . .	29
FIG.4.1	Projetos Servidor e Cliente. . . . .	37
FIG.4.2	Objetivo e Fluxograma do Projeto Eb-CyberDef. . . . .	41
FIG.4.3	Detalhamento de cada módulo do Projeto Eb-CyberDef. . . . .	42
FIG.4.4	Interface de Registro dos Oráculos. . . . .	42
FIG.4.5	Interface de Login. . . . .	43
FIG.4.6	Acesso não autorizado ao listar os tráfegos de rede. . . . .	43
FIG.4.7	Acesso autorizado ao listar os tráfegos de rede. . . . .	44
FIG.4.8	Espera da resposta do servidor com as informações relevantes do <i>log</i> . . .	44
FIG.4.9	Disponibilização das informações relevantes. . . . .	45

## RESUMO

Motivado pelo aumento exponencial no número de serviços que a Internet proporciona à sociedade, em meio a um crescente desenvolvimento da tecnologia e inovação, o homem torna-se cada vez mais dependente da rede. Conseqüentemente, grande parte do foco de atividades ilícitas migrou para o ambiente virtual, cujas brechas ainda permitem boas oportunidades para os infratores. Neste contexto, intensificou-se a necessidade de desenvolver soluções inteligentes para garantir a idoneidade do ciberespaço. Por isso, em conformidade com o que muitas das maiores organizações privadas e governamentais ao redor do mundo vem adotando como premissas de segurança, verificou-se a indispensabilidade, por parte do Exército Brasileiro, de produzir sua própria solução de proteção cibernética. O projeto do EB-CyberDef, de responsabilidade do Instituto Militar de Engenharia, surgiu com este intuito, tendo este projeto de fim de curso a missão de desenvolver um dos componentes de sua estrutura modular. A ferramenta desenvolvida permite, portanto, auxiliar na identificação de tráfegos de rede maliciosos através de uma interface que, ao apresentar algumas de suas características, serve como um painel de apoio à decisão de um analista humano sobre a legitimidade de fluxos suspeitos.

## ABSTRACT

Motivated by the exponential increase in the number of services that the Internet provides to society and inhabiting in a growing technology development and innovation environment, the mankind becomes each time more dependent on the network. As a result, much of the focus of illicit activity shifted to the virtual environment, which intensely exploits the vulnerabilities of constantly deployed new features. In this context, the need to develop smart solutions to ensure the integrity of cyberspace has intensified. Therefore, in accordance with what many of the largest private and governmental organizations around the world adopted as security premises, it is indispensable by the Brazilian Army to develop its own cyber protection solution. The EB-CyberDef project, under the responsibility of the Military Institute of Engineering, came up with this purpose, having this end-of-course project with the mission of developing one of the components of its modular structure. The developed tool thus helps to identify malicious traffic traces through an interface that works as a support panel for a human analyst's to decide on the legitimacy of a suspected network traffic.

# 1 INTRODUÇÃO

Com o advento da chamada Indústria 4.0, nome atribuído ao processo pelo qual estamos vivendo e que, segundo o engenheiro e economista alemão Klaus Schwab, caracteriza a Quarta Revolução Industrial (SCHWAB, 2016), a população mundial tornou-se extremamente dependente da Internet. Sua influência sobre a vida das pessoas é tão forte que não se limita apenas a fornecer novos serviços, mas também está sendo capaz de desenvolver e remodelar diversas práticas e abordagens presentes nos mais variados campos de negócio e conhecimento (SCHWAB, 2016).

Neste contexto de constante inovação, entretanto, surgem simultaneamente inúmeras oportunidades para o desenvolvimento de práticas ilícitas e, tamanha importância que adquiriu, o ciberespaço é um dos principais focos destas atividades. Prova disso é que o número de ataques dentro da rede global vem crescendo exponencialmente no passado recente (ENTREPRENEUR, 2018) e as estimativas apontam para que este multiplicador continue agindo nos próximos anos (VENTURES, 2017a). Considerando apenas ataques de ransomware, por exemplo, verificou-se um aumento de 350% em 2018 (WEEK, 2018) e estima-se que a quantidade de ataques ao setor de saúde, área que pela necessidade de digitalização de dados críticos atrai significativo número de infratores que enxergam uma possibilidade de obter compensação financeira em troca da devolução das informações roubadas, quadruplicará entre 2017 e 2021 (VENTURES, 2017b).

Assim, visto o prejuízo que estas ações podem gerar aos seus destinatários, sejam eles organizações governamentais ou privadas e até mesmo pessoas físicas, cresce também a conscientização sobre a importância de se obter soluções inteligentes que previnam ou diminuam sua eficiência (FORBES, 2018). Neste sentido, o mercado de segurança cibernética, um nicho de mercado relativamente pequeno e sem a atuação de muitas empresas, vem alcançando um crescimento sólido ao longo dos últimos anos, desenvolvendo-se rapidamente e com perspectivas de tornar-se, doravante, ainda mais demandado e disputado. Estima-se que em 2023 será um segmento de mercado que obterá receitas no valor de 250 bilhões de dólares, atingindo até lá um crescimento de aproximadamente 11% ao ano (WATCH, 2018).

## 1.1 MOTIVAÇÃO

O cenário atual onde chegaram os números relativos a crimes no ciberespaço chama atenção de uma parcela da população pelo alto poder de gerar prejuízos financeiros. Conforme relatório mais recente divulgado pela Internet Society's Online Trust Alliance, uma organização global que se destina, principalmente, a promover a evolução e o uso da Internet para o benefício de toda a sociedade global, e para isso se envolve ativamente na questão da segurança da rede (SOCIETY, 2019b), estima-se que a indústria de crimes cibernéticos atingiu no ano de 2018 um valor de 45 bilhões de dólares, quantia correspondente, em apenas um ano, a mais de um terço do número total de ataques realizados desde 2013 (SOCIETY, 2019a). Um outro ponto levantado pelo mesmo relatório, entretanto, refere-se à grande parcela deste total que poderia ter sido evitada: 95% das violações foram consideradas neste grupo passível de prevenção. Dessarte, realça a importância da difusão da preocupação em adquirir defesas contra estes delitos, assim como a criação de novas soluções (SOCIETY, 2019a).

Além disso, verifica-se anualmente um aumento no número de ataques denominados “zero-day” (os quais caracterizam-se por serem crimes que exploram vulnerabilidades até então desconhecidas e, por isso, possuem uma grande capacidade em gerar danos de maiores proporções) e estima-se que até 2021 este crescimento poderá acontecer de forma significativa (STRATUS, 2018). Conseqüentemente, contabiliza-se que soluções padrões em segurança, como os tradicionais antivírus, conseguem deter cada vez menos as novas investidas maliciosas (SECURED, 2018), sendo portanto extremamente importante, a fim de garantir a integridade do ciberespaço, o desenvolvimento de sistemas robustos de detecção de padrões maliciosos. Infraestruturas estas apoiadas no avanço da área de Inteligência Artificial (SECURED, 2018), a qual ganha gradativamente o espaço de técnicas que vem sendo menos efetivas, como a detecção por assinatura, nesta luta pela segurança.

## 1.2 OBJETIVO

O objetivo do presente trabalho é desenvolver um dos módulos do sistema EB-CyberDef, cujo propósito é gerar uma central de detecção de padrões maliciosos para uso, em princípio, do Exército Brasileiro. A elaboração deste módulo consiste em desenvolver um painel de apoio que permitirá a um analista humano (oráculo) decidir sobre a legitimidade de um determinado tráfego de rede.

Os fluxos que serão submetidos à análise do oráculo estarão identificados como sus-

peitos, ou seja, embora fossem aplicadas anteriormente outras técnicas, não concluiu-se a respeito do dado em questão ser malicioso ou não. Dessa forma, é esperado que a informação seja apresentada junto a algumas de suas características consideradas relevantes para contribuir no processo decisório do analista.

### 1.3 JUSTIFICATIVA

Embora o mercado de segurança cibernética esteja vivenciando uma expansão exponencial, inclusive dentro do Brasil, onde diversas empresas se desenvolvem e apresentam vultosos crescimentos (VALOR, 2018), as soluções existentes ainda são, preponderantemente, estrangeiras. Diversos sistemas e serviços utilizados, se já não contratados diretamente de empresas oriundas de outros países, são fornecidos por empresas nacionais que, para desenvolver seu produto, utilizam-se de tecnologia estrangeira. No âmbito da Estratégia Nacional de Defesa, onde o Exército Brasileiro (EB) se insere como principal responsável por garantir a segurança cibernética da nação e de toda sua estrutura crítica, isso certamente configura um perigoso paradoxo: defender seu ciberespaço de ameaças exteriores ao território brasileiro por meio do suporte fornecido por tecnologias desenvolvidas também externas a ele.

Para que isso não aconteça, percebeu-se a necessidade de direcionar parte dos gastos governamentais ao desenvolvimento deste tipo de tecnologia, objetivando a geração de soluções próprias, internas ao país e às suas instituições, para obter uma proteção mais confiável da sua rede. É o que se verifica em outros Estados. Os Estados Unidos, por exemplo, dono de uma importante posição geopolítica e detentor de inúmeras das maiores empresas globais, e por isso um grande foco de crimes do ciberespaço, ao divulgar a estimativa de seu balanço para o ano fiscal de 2019, apresentou um novo aumento na receita destinada às práticas relacionadas à segurança cibernética. O documento prevê uma alocação de 15 bilhões de dólares para estas despesas, um aumento de quase 0,6 bilhão de dólares frente ao ano anterior, divididos pelos diversos departamentos, mas destinados majoritariamente ao seu Departamento de Defesa (HOUSE, 2018).

Nasceu, portanto, com este intuito, o EB-CyberDef, um projeto que visa criar um ambiente integrado de defesa cibernético próprio, para apoio à detecção e ao combate de comportamentos maliciosos no tráfego de redes de computadores. Uma solução em segurança cem por cento brasileira, elaborada e produzida exclusivamente pela sua força terrestre, cujo desenvolvimento deu-se origem por meio da iniciativa da seção de Engenharia de Computação do Instituto Militar de Engenharia em responsabilizar-se pela

confeção deste projeto (EB, 2017).

## 1.4 METODOLOGIA

A metodologia adotada para realizar os objetivos propostos foi composta de quatro etapas: estudo dos fundamentos teóricos, modelagem, implementação e testes.

Em um primeiro momento, a etapa relativa à fundamentação teórica consistiu em estudar sobre noções básicas relacionados à segurança cibernética, assim como funcionamento e características de uma Botnet, conceito fundamental para o desenvolvimento do projeto. Em um estágio posterior, o foco esteve em entender sobre quais características de um tráfego de rede seriam relevantes para serem utilizadas no desenvolvimento do sistema, ou seja, aquelas que apresentam-se como boas candidatas a serem analisadas em um processo decisório que visa marcar o fluxo em questão como malicioso ou não.

Posteriormente, durante a etapa de modelagem, estando consolidada a teoria a ser utilizada na elaboração do trabalho, buscou-se levantar quais os requisitos necessários ao desenvolvimento do projeto, assim como idealizar uma estrutura de classes para o sistema.

Em seguida, a terceira etapa foi destinada a implementar e desenvolver as primeiras versões do projeto, assim como concluir as versões finais após os pareceres dados sobre as anteriores. Maiores detalhes serão abordados em um capítulo adiante deste documento.

Por fim, a última fase foi direcionada a testar os programas desenvolvidos, logo após o término da implementação de cada uma das versões, de modo que todas as restrições previstas na etapa da Modelagem fossem atendidas.

## 1.5 ESTRUTURA DO TEXTO

O presente projeto está organizado em mais 4 capítulos. No capítulo 2 é apresentada uma fundamentação teórica acerca de conceitos importantes relacionados à segurança, essenciais à compreensão do tema abordado no projeto. No capítulo 3 é apresentado de forma resumida o Projeto EB-CyberDef, fornecendo detalhes sobre suas características e especificações. O capítulo 4 apresenta a modelagem utilizada no sistema e decisões de implementação tomadas no projeto. Por fim, no capítulo 5 são apresentadas as considerações finais.



## 2 FUNDAMENTAÇÃO TEÓRICA

Em uma época onde as pessoas chegam a gastar mais de duas horas diárias apenas nas suas redes sociais, um aumento de 50% em relação ao número verificado 6 anos atrás (WORLD, 2019), e onde a tecnologia proporciona cada vez mais o surgimento de novas formas de oferecer serviços, substituindo a necessidade da presença do consumidor pela digitalização do processo (FOLHA, 2019), os dados pessoais que trafegam pela Internet adquiriram um valor imensurável. Neste contexto, o conceito de segurança da informação ganha notoriedade em meio à população, que já se conscientiza sobre a necessidade de obter mecanismos de defesa contra os diversos ataques cibernéticos que surgiram nos últimos anos.

### 2.1 CONCEITOS IMPORTANTES

A primeira definição a ser mencionada deve ser, indubitavelmente, aquela que descreve o ambiente ao qual este tema se refere. Dessa forma, o Ciberespaço caracteriza-se por ser a área de ação das redes de comunicação computadorizadas (MICHAELIS, 2019a), um universo virtual que engloba inúmeros meios de comunicação e interações sociais. Espaço onde se encontram quantidades expressivas de dados, informações e conhecimento, e cujas inovações já permitem a realização de transações econômicas e comerciais, tendo a Internet como sua base operacional (MONTEIRO, 2007). Também chamado de espaço cibernético.

A seguir, buscando-se entender a dinâmica de colocar este ambiente virtual em risco, pode-se explicar o conceito de Ataque Cibernético: também chamado de ciberataque, é uma ação que não envolve danos físicos (TABANSKY, 2011), sendo caracterizada por ser uma tentativa maliciosa e deliberada de um indivíduo ou organização de violar o sistema de informação de algum outro indivíduo ou organização. Normalmente, o responsável pela ação procura algum tipo de benefício por interromper a rede da vítima (CISCO, 2019a). Este agente pode ser definido como Atacante e, no contexto em que o presente trabalho se enquadra, tal termo será utilizado quando desejar referir-se à pessoa ou instituição responsável por um ataque cibernético. Geralmente, a expressão remete a um criminoso do ciberespaço, muitas vezes também chamado de hacker.

Seguindo com as definições, o termo Segurança, no contexto da Segurança de Informação, refere-se ao processo que envolve justamente a proteção dos dados, corporativos

ou pessoais, contra a grande variedade de ataques, tanto cibernéticos quanto físicos, que podem comprometer a confidencialidade, integridade e disponibilidade destas informações e recursos de informações (REID; VAN NIEKERK, 2014). Já quando refere-se ao ciberespaço, é conhecida como Segurança Cibernética a prática de proteger sistemas, redes e programas contra os ciberataques (CISCO, 2019b). Entretanto, estas duas definições são geralmente usadas de forma intercambiável na literatura (REID; VAN NIEKERK, 2014).

Além disso, enquanto o conceito de Ameaça, no contexto cibernético, é qualquer possibilidade de comprometer a segurança e seus pilares de determinada máquina, rede ou sistema, entende-se por Vulnerabilidade a característica de algo que apresenta falhas ou simplesmente o estado do que é vulnerável (MICHAELIS, 2019b). A ameaça geralmente está relacionada a algum tipo de ataque, podendo este situar-se no seguinte domínio de ataques: patrocinados por Estados; consequentes de extremismo ideológico ou político; oriundos de criminalidade ideológica; ou até mesmo vindo de atividades maliciosas individuais. Já o conceito de vulnerabilidade, no contexto cibernético, está relacionado à existência de uma fragilidade em um ativo capaz de ser explorada por uma ou mais ameaças. Esta brecha pode ser originada por três tipos de erros: de projeto, de implementação ou de configuração.

A Defesa Cibernética é, portanto, o ato de proteger-se contra ciberataques, utilizando-se para isso métodos tecnológicos a fim de identificar uma invasão ilícita e sua origem, assim como avaliar os danos causados, impedir sua disseminação e, se necessário, restaurar os dados e reparar as máquinas afetadas. Seu objetivo principal reside na tentativa de estabelecer-se como uma barreira à penetração não autorizada, de maneira a frustrar os propósitos do atacante. (TABANSKY, 2011) E, assim, a Guerra Cibernética é um tipo de guerra onde as ações são realizadas no ambiente do ciberespaço, em especial a Internet e suas redes relacionadas. É caracterizada militarmente como uma combinação de ataques a redes de computadores e defesas destas redes, tendo na informação trafegada o principal elemento explorado e manipulado por estas atividades (DUTRA, 2007). Utiliza, dessa forma, meios informáticos para promover uma situação de espionagem ou uma invasão proibida à uma rede ou equipamento (NUNES, 2012).

Por fim, qualidade de algo que é legítimo e, portanto, legal, amparado pela lei, o termo legitimidade será utilizado no contexto do presente trabalho para referir-se ao nível de segurança presente em um equipamento físico, em uma estrutura de rede ou em um dado trafegando por ela. Consequentemente, algo legítimo corresponderá a algo seguro, não malicioso, enquanto alguma coisa cuja segurança sabidamente fora violada, considerada portanto maliciosa, será igualmente considerada sendo não legítima. Neste sentido,

dessarte, a expressão análise de legitimidade será utilizada quando forem aplicados métodos a fim de se analisar a legitimidade da organização lógica ou equipamento físico em questão, objetivando determinar o quão segura é a estrutura analisada.

## 2.2 TIPOS DE ATAQUE

A fim de detalhar parte das ameaças existentes no ciberespaço, o presente trabalho aborda sobre alguns aspectos de quatro dentre os principais métodos de ataques existentes atualmente, dando especial ênfase ao subtópico referente à Botnet, cuja importância merece destaque por configurar-se como o alvo central do mecanismo de detecção que o projeto EB-CyberDef visa implementar.

### 2.2.1 ENGENHARIA SOCIAL

Caracterizada por explorar a maior vulnerabilidade existente na cadeia de segurança de um sistema - o homem -, a engenharia social é um tipo de ataque onde o atacante atua sobre o ser humano e não explorando falhas de segurança do software ou equipamento em questão. Assim, é considerada uma arte de manipular pessoas que, obtendo sucesso, é capaz de induzi-las a fornecer informações ou executar determinadas ações (WEBROOT, 2019). O contato entre vítima e atacante pode ser feito de diferentes formas: fisicamente, através de contato pessoal; pela rede, através de email, redes sociais ou até mesmo sites de vendas; ou qualquer outro meio de comunicação, como telefonemas (TI, 2013). Dentre os principais tipos de ataque de Engenharia Social, destacam-se: Baiting, Phishing, Pretexting, Quid Pro Quo e Tailgating.

No Baiting, o atacante visa despertar a curiosidade da vítima por meio da exposição de algum dispositivo físico. Este, geralmente hospedando algum tipo de malware, serve de isca para o ataque ao instigar a pessoa a utilizá-lo e, assim, infectar o alvo (PROOF, 2017). No que lhe diz respeito, o Phishing é um ataque muito comum que visa o roubo de dados sigilosos e informações pessoais, a fim de obter alguma vantagem na aquisição deste conhecimento, como ganhos financeiros. Nele, o atacante incita a vítima a acessar alguma página falsa ou link malicioso, responsável pela infecção. A técnica de persuasão consiste em enviar alguma mensagem supostamente idônea, onde o hipotético remetente e origem da notificação possua alguma relação com a pessoa alvo do ataque, de modo que a vítima não suspeite (PROOF, 2017).

O Pretexting, por sua vez, é um ataque onde se cria uma situação falsa visando a conquista da confiança da vítima. Baseado neste pretexto, portanto, o atacante convence

a vítima a lhe passar informações sigilosas ou, ao menos, que ela exponha estes dados a ele (THROUGH EDUCATION, 2009). Diferentemente do Quid Pro Quo, que envolve uma requisição, à vítima, de informações em troca de alguma compensação oferecida pelo atacante (ENISA, 2016), normalmente um serviço ou um benefício que inclui a execução de determinada ação (INFOSEC, 2019). Sua detecção pode ser facilitada se considerada a assimetria geralmente existente entre a obtenção dos dados e a recompensa oferecida (ENISA, 2016).

Por último, o Tailgating, também conhecido como Piggybacking, é um ataque onde o infrator visa o acesso de uma área restrita, que só é possível adentrar devidamente autenticado. O atacante consegue burlar o controle de acesso atuando em cima do descuido de alguma pessoa cuja presença no local é autorizada, seja seguindo-a e entrando atrás dela ou mesmo enganando-a (INFOSEC, 2019).

### 2.2.2 MALWARE

A partir da etimologia da palavra que dá nome a este tipo de ameaça, conseguimos ter uma simples inferência do que pode se tratar esta técnica: do inglês, “mal” representa “malicious” e “ware” corresponde à “software”. Assim, um ataque de Malware consiste basicamente na infecção de um dispositivo, alvo da ação, com um código malicioso responsável por executar determinadas ações planejadas pelo atacante, geralmente sem o conhecimento da vítima (CYBERSECURITY, 2019).

No decorrer dos anos, com a evolução e diversificação deste tipo de ataque, verificou-se que uma infecção via Malware pode se utilizar de diversos mecanismos para realizar sua investida maliciosa. Desta forma, de acordo com as características e resultados das atividades de cada tipo de código, eles foram classificados em diferentes categorias, dentre as quais as mais comuns são: Adware, Spyware, Vírus, Worms, Trojan, Ransomware, Rootkit, Keylogger, etc (MALWAREBYTES, 2018).

Dentre as formas de Malware comentadas anteriormente, duas podem ser citadas pela recente notoriedade que vem alcançando: o Spyware, responsável por explorar, no primeiro semestre do corrente ano, uma vulnerabilidade existente no aplicativo de troca de mensagens WhatsApp (FASTCOMPANY, 2019), que configura-se atualmente como o aplicativo mais popular deste mercado (INC., 2018; STATISTA, 2019; EXPLOSION, 2019); e o Ransomware, que em 2017 adquiriu grande popularidade ao causar considerável estrago por infectar diversas máquinas em várias partes do globo, por meio de um software que ficou conhecido como WannaCry (TECMUNDO, 2017), e desde então vem

consolidando-se como principal ameaça dentre os ataques de Malware, importância que não deve ser diminuída no ano de 2019 (PHOENIXNAP, 2019).

### 2.2.3 (D)DOS

O ataque de Negação de Serviço (do inglês, Denial of Service) caracteriza-se por almejar a interrupção do correto funcionamento de um computador ou qualquer outro dispositivo alvo da ação. O atacante geralmente procura sobrecarregar a máquina em questão com inúmeras requisições, de forma que comprometa sua capacidade de operação e, assim, ações que ela execute ou serviços que ela provenha sejam indisponibilizados (CLOUD-FLARE, 2018).

Um ataque similar ao DoS é justamente o ataque Distribuído de Negação de Serviço (do inglês, Distributed Denial of Service), cuja execução é baseada nos mesmos princípios do primeiro, porém carrega uma importante diferença em relação a ele: enquanto o DoS utiliza-se de apenas uma máquina para a realização do ataque, a ação no DDoS é realizada utilizando-se uma rede de computadores. Dessa forma, a atividade é distribuída entre diferentes conexões, ou seja, há um número maior de recursos computacionais comprometidos com o ataque, o que proporciona um considerável ganho de resultados quando comparado a um ataque mais simples de DoS (BISEND, 2019).

Dentre os tipos de ataques de negação de serviço mais comuns, podemos citar dois tipos de inundações que afetam os dois principais protocolos da camada de transporte: as inundações SYN e UDP.

A Inundação SYN explora uma falha de projeto já conhecida do protocolo da camada de transporte TCP, que exige o cumprimento de uma sequência pré-estabelecida de troca de mensagens (“Three-Way Handshake”: SYN, SYNACK, ACK) para a abertura de uma conexão. Nele, o atacante envia inúmeras mensagens SYN à máquina vítima do ataque, como se estivesse solicitando a abertura de várias conexões, mas não responde a sua mensagem de resposta SYNACK com o ACK final necessário ao estabelecimento da conexão. Desta forma, compromete o funcionamento do dispositivo, já que ele permanecerá aguardando a terceira e última mensagem do processo, indisponibilizando seus recursos até que uma nova conexão seja feita (IMPERVA, 2015).

Já na Inundação UDP, o hacker envia à vítima inúmeros pacotes UDP em portas de destino aleatórias. Esta ação se baseia no funcionamento do protocolo, no qual a máquina a quem se destina estes pacotes procura por algum aplicativo que esteja ouvindo a porta em questão e, caso não encontre nenhum, responde com uma mensagem ICMP

reportando este erro. Assim, quando são recebidos muitos destes pacotes UDP que não fazem parte de uma comunicação legítima, a vítima irá responder com inúmeros pacotes ICMP notificando tais erros, processo o qual consumirá muitos dos seus recursos. Isto pode, portanto, torná-la indisponível, impedindo que ela responda a solicitações legítimas (IMPERVA, 2015).

## 2.2.4 BOTNET

Conforme discutido em seguida, o conceito de uma Botnet está vinculado ao emprego de um grande número de recursos computacionais para realizar um ataque cibernético, alcançando, assim, considerável escalabilidade na ação maliciosa (KAIO R. S. BARBOSA, 2014). Utilizando-se dela, o planejamento de um ataque pode fazer uso e combinar diferentes técnicas, inclusive as discutidas nas seções anteriores, de forma a obter resultados mais relevantes quando comparado à utilização de cada uma delas separadamente. A Botnet configura-se, portanto, como o método de ataque de maior relevância para o projeto a ser desenvolvido, sendo o foco da teoria estudada no nosso trabalho.

### 2.2.4.1 DEFINIÇÃO

Analisando a etimologia da palavra, não é difícil perceber que sua origem deriva de dois outros termos relacionados à tecnologia que, já há algum tempo, ganharam bastante destaque popular: de “robot” e “network”, que em tradução livre significam robô e rede, surgiram as expressões “bot” e “net”. Caracterizada, assim, por ser um conjunto de máquinas infectadas por determinado malware e que se comunicam entre si sob a obediência de diretrizes provenientes de um ou mais controladores comuns, que fornece a ideia de rede de robôs da qual originou-se o vocábulo, a Botnet representa uma das maiores ameaças à segurança cibernética, responsável por infectar, há anos e no mundo inteiro, um imenso número de dispositivos conectados à Internet (ZHU et al., 2008).

### 2.2.4.2 FUNCIONAMENTO

Seu funcionamento está associado à figura de um atacante, designado botmaster, que por meio de uma infra-estrutura de comando e controle, estabelecida por um ou mais servidores (normalmente denominado Servidor de Comando e Controle, ou simplesmente Servidor C&C), consegue infectar outros dispositivos e, então, controlar e coordenar suas ações. Estas primeiras vítimas são responsáveis por dar prosseguimento ao ataque e, se for o desejo do hacker, continuar com a infecção de novas máquinas. Estas, que foram

infectadas com o software malicioso, são chamadas de bots e comunicam-se entre si e com o botmaster a partir do canal de comunicação criado, a fim de transmitir entre elas e propagar adiante as instruções recebidas dele. Gera-se, assim, uma estrutura de rede de robôs, conforme citado anteriormente. Uma representação de uma típica Botnet é mostrada na figura 2.1.

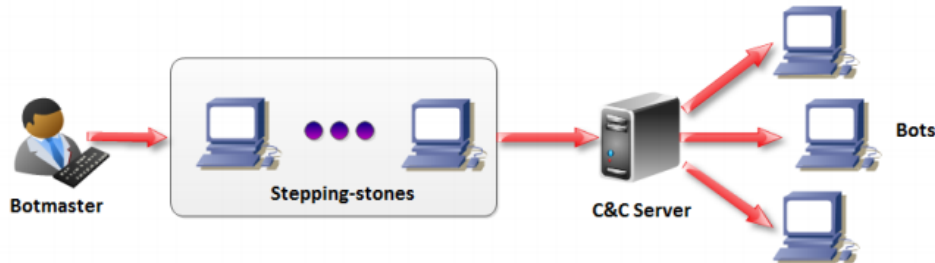


FIG. 2.1: Estrutura de uma típica Botnet. (KHATTAK et al., 2013)

A partir desta rede, portanto, o infrator alcança uma maior eficácia na sua investida maliciosa, já que é capaz de contar com uma maior quantidade de recursos computacionais comprometidos com o objetivo do ataque. Além disso, para os defensores do ciberespaço, lidar com um considerável número de máquinas infratoras, geograficamente e topologicamente distribuídas, torna a missão de garantir proteção mais complexa, exigindo mecanismos mais sofisticados (MARZANO et al., 2018).

Outra vantagem na sua utilização está no fato do comportamento dos bots variar conforme estratégia do botmaster. Afinal, o ataque pode assumir diferentes níveis de visibilidades, propiciando que, simultaneamente à alternativa de assumir o controle total do dispositivo infectado, haja a possibilidade do malware atuar invisivelmente aos usuários, executando de forma silenciosa enquanto aguarda novos comandos do controlador (KHATTAK et al., 2013).

Podemos, assim, justificar o propósito da criação e utilização de uma Botnet em um dado ataque por permitir que o atacante recrute e administre centenas, milhares ou mesmo milhões de máquinas, de forma que suas atuações combinadas proporcionem não só uma grande escalabilidade do prejuízo causado pela atividade maliciosa, como também uma maior dificuldade na detecção e inviabilização do agente criminoso (KHATTAK et al., 2013).

### 2.2.4.3 COMPONENTES

Nesta subseção, segue uma básica explicação acerca das características dos três principais componentes de uma Botnet: o Botmaster, o Servidor C&C e os Bots.

O botmaster é a pessoa ou organização responsável pelo ataque. Ele configura o Servidor C&C e, a partir dele, implementa uma estratégia para sua atividade ilícita. Controla remotamente os bots e os instruem através de comandos nas práticas de atividades maliciosas. Dependendo do seu objetivo, pode optar por uma topologia de rede em particular, obtendo certos benefícios, em detrimento de algumas desvantagens, no caminho do que se deseja alcançar. Para dificultar sua detecção, pode ainda empregar algumas máquinas entre ele e o seu servidor C&C (KHATTAK et al., 2013).

Já o servidor C&C caracteriza-se por ser a interface entre o botmaster e sua rede. Dessa forma, ao ser o ponto de contato entre o atacante e os diversos bots existentes, é por este servidor que ele controla a Botnet, sendo por meio dele também que acontece toda a comunicação entre os dispositivos. A partir dele são lançadas novas ordens a serem executadas, do botmaster às suas máquinas infectadas, assim como é por ele que os bots enviam notificações e informam sua admissão na rede (MARZANO et al., 2018). É imprescindível que o botmaster invista determinado esforço para proteger o servidor C&C, já que é por meio dele que todas as máquinas pertencentes à Botnet são controladas e, portanto, acaba tornando-se um bom alvo de agentes de segurança ou botmasters concorrentes interessados em detectar e destruir sua rede (VORMAYR et al., 2017).

Por fim, embora denomina-se de bot o software malicioso responsável pela infecção do dispositivo (BAILEY et al., 2009; KAIO R. S. BARBOSA, 2014; UFRJ, 2015), o termo bot é usado igualmente para fazer referência às máquinas infectadas, muitas vezes também chamadas de robôs ou zumbis (KHATTAK et al., 2013; VORMAYR et al., 2017). De ambas as formas, os bots são os responsáveis por executar as ações ordenadas pelo botmaster e, assim, propagar o ataque. Seja roubando informações, infectando novas máquinas, inviabilizando um serviço ou qualquer outra ação maliciosa, eles são os agentes finais da atividade ilícita. Quanto maior o número de bots presentes em uma Botnet, maior quantidade de recursos computacionais à disposição do atacante e, conseqüentemente, maior poder de estrago da Botnet em questão. Os bots comunicam-se entre si e com o botmaster através do canal de comando e controle estabelecido.



#### 2.2.4.4 TOPOLOGIAS DE UMA BOTNET

Dependendo do objetivo da atividade, o atacante precisa tomar alguns cuidados. Afinal, a melhor forma de estruturar sua rede maliciosa pode variar de acordo com o que se deseja. Assim, diferentes formas de organizar geograficamente e fisicamente as máquinas infectadas integrantes da Botnet apresentam-se como alternativas. Elas se dividem basicamente em três grupos: aquelas que apresentam uma arquitetura centralizada, que enxergam o Servidor C&C como um ponto central da comunicação entre os componentes da rede (VORMAYR et al., 2017); aquelas que apresentam uma arquitetura descentralizada, onde não existe a lógica de mestre-escravo entre um único Servidor C&C e os inúmeros bots, permitindo que o gerenciamento da comunicação seja responsabilidade de diversas máquinas distribuídas pela rede (KHATTAK et al., 2013); e as de arquitetura híbrida, que ficam no meio do caminho entre as duas anteriores e buscam mesclar suas características.

Dentre as topologias centralizadas, podemos citar a Topologia Estrela e a Topologia Hierárquica. A primeira possui um único Servidor C&C centralizado, responsável por toda comunicação existente entre o botmaster e os bots. Possui como principal vantagem a simplicidade e a rapidez na comunicação, otimizando a transmissão de comandos. Como desvantagem, destaca-se a existência de um ponto único de falha: estando o Servidor C&C exposto, seu bloqueio ou desabilitação acarreta na neutralização da Botnet (KHATTAK et al., 2013; UFRJ, 2015). A segunda topologia utiliza-se dos bots já pertencentes à rede para contaminação e posterior disseminação das instruções para as novas máquinas infectadas, gerando, assim, uma estrutura de hierarquia. Justamente por prover uma ou mais camadas de bots entre os agentes finais da Botnet e o botmaster, esta topologia não o expõe (KHATTAK et al., 2013). Além disso, fornece uma maior escalabilidade e dificulta a determinação do tamanho de uma Botnet (UFRJ, 2015). Entretanto, acrescenta considerável latência na comunicação devido à obrigatoriedade de passar por algumas camadas de dispositivos (KHATTAK et al., 2013). Uma ideia de sua arquitetura é mostrada na figura 2.2.

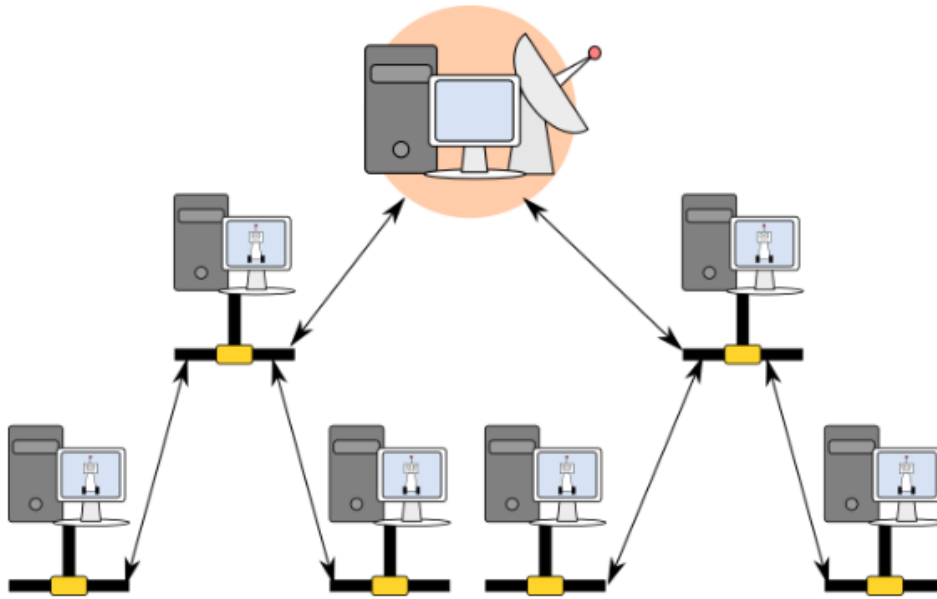


FIG. 2.2: Topologia Hierárquica de uma Botnet. (UFRJ, 2015)

Quanto às topologias descentralizadas, destacam-se a Topologia Multi-servidor ou Topologia Distribuída e a Topologia Peer-to-Peer. A primeira, uma versão estendida e refinada da topologia estrela, caracteriza-se pela existência de, em vez de um único, múltiplos Servidores C&C. Espalhados por diferentes localizações geográficas, cada um deles controla um subconjunto do total de bots, comunicando-se também entre eles mesmos durante a administração da Botnet (KHATTAK et al., 2013). Alcançam certo nível de descentralização ao permitir redundância no gerenciamento da comunicação: se um Servidor C&C for desabilitado, os que restarem ainda serão capazes de manter o canal. Em contrapartida, requer maior esforço e conhecimento do botmaster para construir e manter tal infra-estrutura (UFRJ, 2015). Já a Peer-to-Peer, conforme representada na figura 2.3, caracteriza-se por ser uma topologia randômica, pois não há uma relação de mestre-escravo clara entre Servidores C&C e as máquinas infectadas e, além disso, qualquer bot pode assumir o papel de administrador do canal de comunicação e transmitir instruções para outros bots agentes (KHATTAK et al., 2013). Assim, o modelo de comunicação empregado e a ausência total de um canal de comando e controle centralizado tornam extremamente difícil a localização do botmaster e a queda da botnet. Entretanto, pelo fato de um bot manter uma lista de vários outros agentes, condição necessária para que seja possível implementar esta estrutura descentralizada, a captura de um deles identificará diversos outros. Como outra desvantagem deste tipo, destaca-se também a latência introduzida na comunicação (KHATTAK et al., 2013).

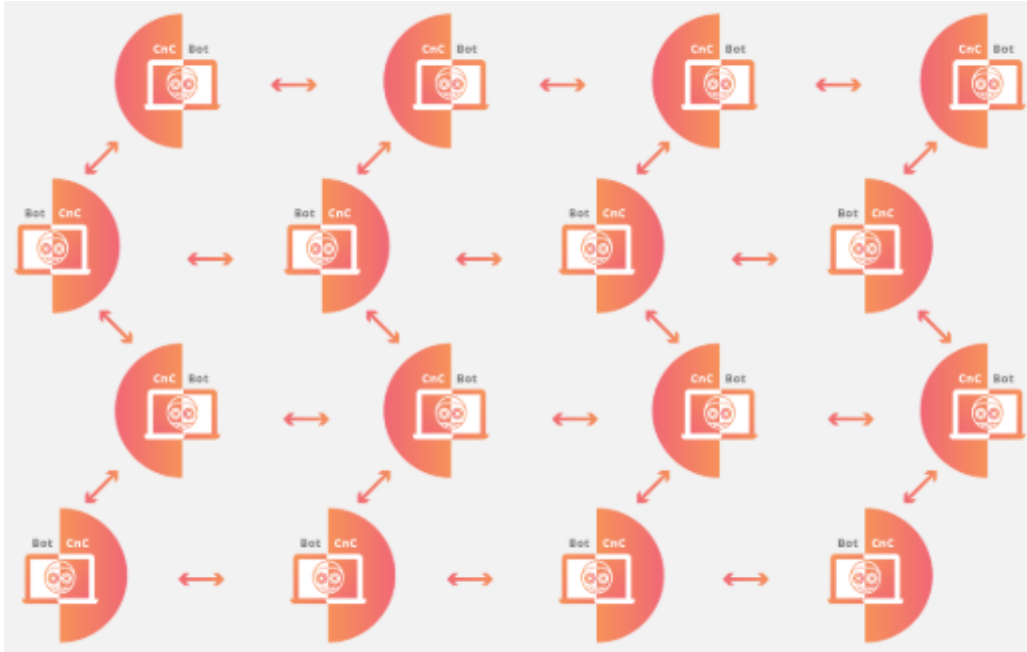


FIG. 2.3: Topologia Peer-to-Peer de uma Botnet. (CLOUDFLARE, 2018)

## 2.3 TÉCNICAS DE DEFESA

À medida que surgem inúmeras formas de ataque, desenvolvem-se novos mecanismos com o objetivo de garantir a segurança do ciberespaço. Nesta corrida tecnológica, diversas ferramentas com diferentes características surgem a fim de diminuir os resultados das ações maliciosas e, assim, abordamos algumas das categorias em que estes mecanismos podem ser classificadas.

### 2.3.1 MONITORAMENTO: DA ESTAÇÃO X DO TRÁFEGO DE REDE

Uma das classificações em que as técnicas de defesa podem ser divididas relaciona-se ao foco da ação defensiva, seja ela preventiva ou corretiva: enquanto umas concentram-se em garantir a integridade de uma máquina em específico, outras são responsáveis por manter seguro um domínio maior de dispositivos, tendo como missão proteger inteira ou parcialmente uma rede.

Um exemplo claro de onde ocorre esta distinção é a ferramenta IDS (do inglês, Sistemas de Detecção de Intrusão), que pode ser dividida em dois tipos: HIDS e NIDS. O primeiro caracteriza um sistema que monitora uma estação em específico, onde se deseja detectar atividades ameaçadoras à sua segurança. Para isso, ele verifica constantemente os arquivos da máquina em questão e mantém registro do tráfego que é destinado ou originado por ela. O segundo por sua vez é responsável pelo monitoramento do tráfego

existente em uma rede ou parte dela, gerando registros e analisando os pacotes que são repassados entre seus diversos componentes (VINCHURKAR; RESHAMWALA, 2012).

O projeto em que o presente trabalho se insere visa o desenvolvimento de uma ferramenta capaz de monitorar uma rede e não apenas uma estação, analisando todo seu tráfego e tendo a aptidão para identificar padrões maliciosos que passam por ele.

### 2.3.2 DEFESA: PASSIVA X ATIVA

Embora estas duas categorias de defesa visem a integridade da rede de quem as emprega, bem como dos dados sob sua posse, a diferença de atuação entre elas é nítida. Os métodos passivos caracterizam-se como a base da proteção existente em um sistema, a fim de minimizar os danos ou reduzir a probabilidade de ocorrência de um ataque cibernético. São mecanismos mais simples, que impõem uma camada básica de proteção e não possuem a intenção de reagir a um ataque após sua ocorrência e tentativa de reparo (LACHOW, 2013).

Em contrapartida, os métodos ativos buscam atuar em cima de cada ação maliciosa, reagindo sempre que possível. São baseados em coleta contínua de informações, a fim de melhor compreenderem as investidas maliciosas e adequarem sua defesa de forma a prevenir a rede contra ações futuras, atualizando-se constantemente para isso. Podem também, a partir do reconhecimento de determinado ataque, disseminar mecanismos de reparo pela rede, buscando desinfetar máquinas atingidas, assim como lançar ofensivas contra o atacante, de modo que além de neutralizar a investida atual consiga evitar novas ações futuras (XU et al., 2015).

### 2.3.3 DETECÇÃO POR: ASSINATURA X COMPORTAMENTO

Todas as vertentes de estudos sobre técnicas de detecção de malwares subdividem-se nestes dois tipos. A primeira, baseada em assinaturas de código-fonte, permite a detecção por meio de uma análise estática. A segunda, baseada no comportamento de uma aplicação, requer por sua vez uma análise dinâmica dela (RIBEIRO, 2017). Enquanto na estática a análise é feita sem a execução do arquivo, na dinâmica a análise é realizada enquanto o arquivo está sendo executado (CHUMACHENKO, 2017).

A detecção por assinatura consiste em procurar dentro do programa suspeito a ser analisado uma cadeia de caracteres que sabidamente caracteriza a aplicação como maliciosa. Esta sequência de bytes, definida por assinatura, é gerada extraíndo-se uma parte do código de um programa que previamente sabe-se pertencer a um malware e que, além

disso, seja dificilmente encontrada no corpo de algum outro programa, de forma a associar com exatidão a aplicação analisada a este malware específico. Devido a esta correspondência exata, o emprego destas técnicas geram poucos falsos positivos. Contudo, há dois fatores, relacionados ao fato das técnicas de ataque estarem sempre se atualizando e originando novas versões de códigos maliciosos, que podem tornar a utilização delas não tão vantajosa. O primeiro diz respeito ao tamanho da base de assinaturas mantida, que requer nova entrada no banco a cada nova versão criada. O segundo diz respeito à eficácia do método, visto que ele não consegue identificar um malware cuja assinatura não foi ainda mapeada e, assim, uma grande frequência no surgimento de novos tipos desta ameaça, como vem sendo verificado atualmente, torna a base de assinaturas desatualizada e pouco eficiente (MARTINS, 2017).

Na detecção por comportamento, a conduta do malware é monitorada enquanto ele é executado, de modo que se atente para sinais de comportamento malicioso, como determinadas modificações no sistema ou estabelecimento de conexões suspeitas (CHUMACHENKO, 2017; MARTINS, 2017). Analisado separadamente, cada um deste sinal suspeito pode não induzir a uma ameaça real, mas a combinação deles pode convergir para um diagnóstico malicioso, o que realça a importância de esforçar-se na implementação de métricas relevantes para a identificação do ataque (CHUMACHENKO, 2017). O principal benefício nesta técnica, e o que torna a sua utilização imprescindível junto à técnica baseada em assinatura, é o seu potencial para identificar novos ataques. Configura-se, assim, como uma etapa complementar àquela anteriormente citada ao detectar episódios de invasão até então desconhecidos, capacidade vital em um cenário que novos tipos de ameaças são desenvolvidos a um ritmo acelerado. Entretanto, uma das suas desvantagens quando comparada com a técnica anterior, reside na sua quantidade de erro ao julgar um comportamento como anormal, dada a maior subjetividade presente neste segundo processo. Possui, portanto, geralmente uma taxa de falsos positivos mais alta do que àquelas em sistemas baseados em assinatura (GARCÍA-TEODORO et al., 2009).

### 3 EB-CYBERDEF

#### 3.1 INTRODUÇÃO AO PROJETO

O EB-CyberDef é um projeto da seção de Engenharia de Computação do Instituto Militar de Engenharia e que tem como objetivo geral desenvolver um protótipo de um ambiente computacional para apoio à detecção e ao combate de comportamentos maliciosos no tráfego de redes de computadores.

O projeto se justifica no contexto do Exército Brasileiro (EB) pelo fato de apresentar-se como uma solução própria a ameaças que podem comprometer de forma significativa o funcionamento do Estado brasileiro e suas instituições. Desse modo, permitirá que se trabalhe isoladamente com os dados coletados, informações obtidas e resultados gerados, o que é essencial por tratar-se de um tema de alta criticidade e com bastante conteúdo sensível. Além disso, será um produto que propiciará um acompanhamento do desempenho das soluções implementadas e a manutenção de um registro do que se considerar necessário, possibilitando um futuro reuso das informações. Torna-se, portanto, imprescindível para as atuais aspirações da Estratégia Nacional de Defesa em consolidar-se como uma nação independente no âmbito da segurança cibernética, ademais quando considerada a carência que esta área ainda possui de uma infra-estrutura que forneça suporte a experimentos e que permita lidar com a imensa quantidade de dados existentes.

Dessa forma, espera-se que os resultados do projeto possam: viabilizar o início da construção de uma base de conhecimento nacional, que possa futuramente ser estudada pelo EB, sobre padrões de comportamentos maliciosos em redes de computadores; fornecer subsídios que auxiliem o corpo técnico da força na formulação de uma política nacional de combate a tais condutas suspeitas nestas redes; e contribuir para a disseminação deste importante conhecimento dentro de outras organizações do Exército ou até mesmo em outras instituições relacionadas.

#### 3.2 ESTRUTURA DO PROJETO

A arquitetura do projeto é dividida em 9 módulos, cada qual com sua função perante o funcionamento integral do sistema, conforme ilustrado na figura 3.1 e descritos a seguir:

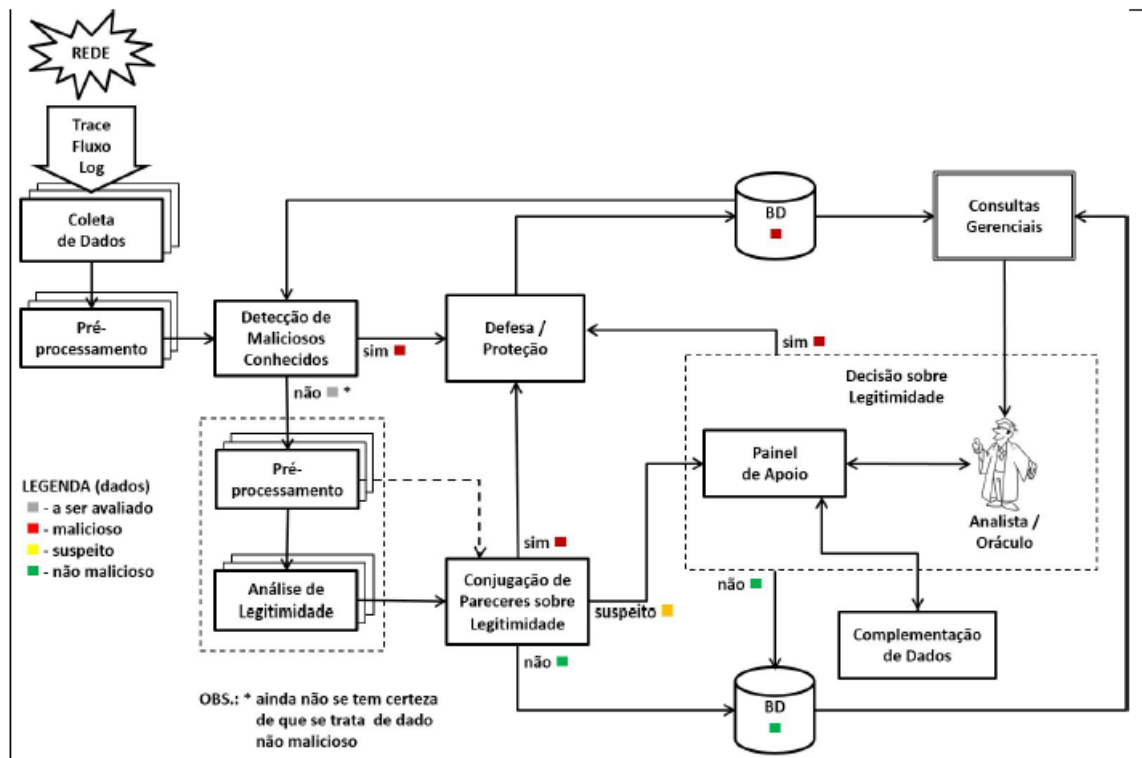


FIG. 3.1: Visão Macro-Funcional da Arquitetura da Fase de Produçã/Operacão do EB-CyberDef.

- Coleta de Dados

O módulo de coleta dos dados da rede deve ser capaz de extrair informações de diferentes fontes de dados (traces, logs e fluxos) em vários formatos.

- Pré-processamento

Este módulo compreende operacões de tratamento e padronizacão dos dados de redes coletados, de forma a prepará-los para serem processados pelo sistema.

- Detecçã de Maliciosos Conhecidos

Módulo responsável pela identificacão dos dados maliciosos conhecidos (marcados como vermelhos, conforme figura 3.1) através de sua assinatura, isto é, características do código malicioso que podem ser percebidas sem a necessidade de mecanismos baseados em Inteligência Artificial e Aprendizado de Máquina. Este módulo, portanto, utiliza a técnica de detecçã baseada em assinatura para realizar uma primeira filtragem dos logs coletados e pré-processados.

- Defesa/Proteção

Confirmado que determinado fluxo é malicioso, este módulo deve acionar medidas de defesa e/ou proteção para mitigar o problema. Tais medidas são denominadas Funções de Proteção. Estas funções podem ser especializadas para firewalls, servidores e roteadores. Um exemplo de medida preventiva que pode ser tomada é a adição de uma regra em um firewall com o objetivo de bloquear, exclusivamente, o fluxo malicioso. Conforme Visão Macro-Funcional da arquitetura, exposta na figura 3.1, observa-se que os logs de entrada para este módulo podem ser direcionados a ele em três momentos distintos do processo, após cada uma das etapas responsáveis por decidir se o fluxo é malicioso ou não. Além disso, este módulo é responsável por enviar um registro deste tráfego identificado como malicioso ao banco de dados responsável por manter estes logs (vermelho), de modo que estas informações sejam reutilizadas por outros módulos do sistema.

- Pré-processamento e Análise de Legitimidade

Este módulo compreende a execução de algoritmos inteligentes de análise de legitimidade dos dados, responsáveis por avaliar os padrões de dados, procurando classificá-los quanto ao seu potencial em se constituir um padrão malicioso. Ou seja, ele utiliza a técnica de detecção baseada no comportamento da aplicação, tendo como entrada os logs marcados como a ser avaliados (cinzas, aqueles que em um primeiro momento não foram identificados como maliciosos, de acordo com a figura 3.1) pelo módulo Detecção de Maliciosos Conhecidos. Cabe ressaltar que a execução dos algoritmos de análise de legitimidade pode ser precedida de diferentes processamentos que irão adequar (pré-processar) os dados conforme a necessidade de cada algoritmo.

- Conjugação de Pareceres sobre Legitimidade

Este módulo tem como propósito integrar os pareceres emitidos pelos algoritmos de legitimidade executados pelo módulo anterior, sobre os fluxos que ainda não se tem certeza de que se trata de dado não malicioso, a fim de obter um parecer único que reflita a impressão do sistema quanto à classificação do padrão analisado. Desta forma, o presente módulo deve classificar os dados em (i) certamente não maliciosos (verde), (ii) certamente maliciosos (vermelho) e (iii) suspeito (amarelo). Os dados marcados como verde devem ser enviados a um banco de dados responsável por armazenar tais fluxos não maliciosos. Os dados em vermelho serão enviados ao módulo Defesa/Proteção, abordado anteriormente. A última classificação deve refletir situações em que o sistema não consiga identificar com clareza se o dado é malicioso ou não, sendo este enviado ao módulo de Painel de Apoio.



- Painel de Apoio

O módulo de Painel de Apoio tem como objetivo apresentar a um analista humano (oráculo) os resultados da conjugação de pareceres de legitimidade dos fluxos marcados como suspeitos. Diante dos dados apresentados, o oráculo deverá opinar sobre a situação do padrão apresentado e indicar como tal padrão deverá ser tratado pelo sistema. É requisito da interface a ser desenvolvida apresentar também características (destes tráfegos suspeitos) consideradas relevantes ao processo decisório do analista, servindo como um auxílio à sua tomada de decisão. Além disso, caso o oráculo deseje, o painel de apoio poderá apresentar, com o mesmo intuito de ajudar no julgamento, dados externos ao sistema.

Este módulo é o foco do presente trabalho, que tem como objetivo o desenvolvimento desta interface, bem como o levantamento destas características responsáveis por auxiliar o processo decisório.

- Complementação de Dados

Módulo responsável por obter dados externos ao sistema que serão apresentados pelo Painel de Apoio. Conforme seu nome sugere, o módulo de complementação dos dados deve realizar buscas inteligentes cujo resultado possa ser útil para a avaliação do oráculo.

- Consultas Gerenciais

Este módulo compreende a exibição de relatórios e consultas gerenciais sobre o comportamento do sistema, permitindo monitorar a qualidade dos resultados encontrados e assim facilitar um eventual ajuste dos parâmetros do sistema a ser realizado na fase de experimentação/configuração.

## 4 MÓDULO PAINEL DE APOIO

### 4.1 OBJETIVO

O objetivo dessa seção é listar quais são as *features* de um tráfego de rede relevantes a serem extraídas, explicar como cada uma impacta no processo decisório da legitimidade de um determinado fluxo de rede, expor a motivação das escolhas de cada ferramenta utilizada para desenvolver o painel de apoio e explicitar a forma com a qual o projeto foi estruturado e implementando.

### 4.2 FEATURES RELEVANTES

Esse tópico tem como objetivo apresentar quais *features* de um tráfego de rede são relevantes para contribuir no processo decisório da legitimidade do mesmo, apresentando-se, assim, como boas candidatas a embasarem o oráculo.

#### 4.2.1 PARECER DO MÓDULO DE PRÉ-PROCESSAMENTO

O módulo de pré-processamento e análise de legitimidade é responsável por avaliar os padrões dos dados recebidos e responder, para cada algoritmo inteligente utilizado, um valor que representa o quão perto de um comportamento malicioso o fluxo de rede avaliado se assemelha. Desta maneira essa informação pode ter papel fundamental na decisão do oráculo, pois explicita o quão perto de um potencial malicioso determinado *log* se encontra.

#### 4.2.2 NOME DE DOMÍNIO

Essa informação serve para facilitar a memorização dos endereços na Internet, dessa forma sítios legítimos se preocupam em definir o seu domínio com palavras significativas e que remetem à informações do conteúdo que será apresentado, para assim, criar uma rápida assimilação do site com o cliente. Portanto, um nome de domínio com uma sequência de caracteres sem significado pode caracterizar um fluxo malicioso, no qual o atacante não se preocupou em disfarçar o domínio.

### 4.2.3 DATA DE REGISTRO DO DOMÍNIO

Os nomes de domínio são registrados normativamente por um ou mais anos e fielmente renovados a partir de então. Domínios destinados a ataques cibernéticos, no entanto, são registrados, rapidamente utilizados para o ataque e abandonados, dessa maneira caracterizando-se voláteis. Mais de 70% dos domínios recém registrados são classificados como "maliciosos" ou "suspeitos" (CHEN, 2019). Portanto essa informação pode ser decisiva para determinar a legitimidade de determinado tráfego.

### 4.2.4 GEOLOCALIZAÇÃO

A informação da localização do endereço de IP remoto pode ser de suma importância para o processo decisório do oráculo, visto que determinados lugares são mais comumente caracterizados como potenciais origens de ataques maliciosos. Em 2017, por exemplo, 20% dos cyberataques possuíram origem na China, 11% nos Estados Unidos e 6% na Rússia (SOBERS, 2019),

### 4.2.5 TIPO DO CONTEÚDO DE RESPOSTA

Como visto anteriormente, em ataques de Botnet, são utilizados servidores de comando e controle, cuja função é controlar, via comandos presentes em arquivos de tipo de conteúdo *text/plain*, os *bots*. Dessa maneira fazer a verificação do tipo de arquivo retornado pode auxiliar o oráculo a detectar esses tipos de ataque.

### 4.2.6 TOP LEVEL DOMAIN

A extensão de um domínio identifica algo sobre o site associado a ele, como seu objetivo, a organização que o possui ou a área geográfica de origem. Cada *Top Level Domain* possui um registro separado, gerenciado por uma organização designada, sob a direção da Internet Corporation para nomes e números atribuídos. Caso essa extensão não represente organizações conhecidas, como as militares e ONG's, ou não seja de alguma localidade geralmente utilizada, isso pode caracterizar um ataque suspeito.

### 4.2.7 PRESENÇA DO DOMÍNIO EM *BLACKLISTS*

Várias organizações mantêm e publicam listas de bloqueio de endereços IP e URL's suspeitos de atividades maliciosas, portanto ter ciência se determinado endereço está contido em alguma *blacklist* pode ser decisório para definir esse fluxo como malicioso.

## 4.2.8 INFORMAÇÕES GERAIS ACERCA DO FLUXO DE REDE

A apresentação das informações do fluxo de rede, tais como a porta utilizada na comunicação, a data que o *log* foi gerado e o endereço de IP do cliente que realizou a requisição podem ser de suma importância para o oráculo tomar a sua decisão, visto que são características inerentes da comunicação realizada.

## 4.2.9 INFORMAÇÕES RELATIVAS À REQUISIÇÃO HTTP

Não só o tipo do conteúdo respondido pelo servidor na comunicação baseada no protocolo HTTP, pode ser utilizado pelo oráculo. Dados como o tempo de resposta, o *status code* retornado e o tamanho da resposta podem também dar indicativos importantes para a decisão do oráculo.

## 4.2.10 REGISTRO DO DOMÍNIO

Ter conhecimento sobre quem registrou e o local de registro do domínio também pode ajudar no momento de decisão da legitimidade do *log*, visto o oráculo pode perceber que a instuição que realizou o registro é conhecida ou que o local de registro é incomum.

## 4.3 FERRAMENTAS

### 4.3.1 LINGUAGENS DE PROGRAMAÇÃO

As linguagens de programação são um conjunto de regras sintáticas e semânticas usadas para comunicar instruções substanciais para o computador. Essas regras apresentam notações matemáticas e, na maioria das linguagens definidas como de alto nível, uma semântica similar ao inglês, de forma que os compiladores de cada linguagem, ou programas tradutores, realizem a conversão desse texto padronizado para a linguagem de máquina (DEVMEDIA, 2012).

#### 4.3.1.1 PYTHON 3

A linguagem de alto nível escolhida para desenvolver o servidor do projeto foi Python 3. Por ser uma linguagem pouco verbosa, dinâmica, assim apresentando-se bem flexível, e de rápida prototipagem, a comunidade de programadores vem adotando essa linguagem cada vez mais nos últimos anos, de forma que em 2019 atingiu o patamar de segunda linguagem de programação mais utilizada pelos desenvolvedores (STACKOVERFLOW,

2019), perdendo somente para o JavaScript, linguagem a qual foi utilizada para desenvolver o *frontend* do projeto. Dessa maneira diversas bibliotecas *open source* vem sendo implementadas, com *features* novas e melhorias, mais um fator que influenciou essa escolha, pois assim, a linguagem acompanha o rápido e contínuo desenvolvimento de novas tecnologias. A escolha da versão 3 ao invés da versão 2 se dá por dois principais motivos, primeiramente pois a versão 2 será descontinuada no ano de 2020 e pelo fato de uma melhoria considerável na principal biblioteca responsável pelas chamadas assíncronas (*asyncio*), fundamental para esse projeto.

#### 4.3.1.2 ECMAScript 6

O ECMAScript é a descrição formal e estruturada da linguagem que o JavaScript implementa e a partir da sexta versão o ECMAScript se consolidou na comunidade de desenvolvedores por se apresentar de forma mais enxuta, flexível e como Java e Python, orientada a objeto (IMASTERS, 2017). A escolha dessa linguagem para implementar a interface se deve também pelo fato de os arquivos interpretados pela maioria dos browsers serem arquivos JavaScript.

### 4.3.2 WEB FRAMEWORKS

Um *Web Framework* provê ferramentas para suportar e implementar um serviço na *Web*. O objetivo de um *Framework* é automatizar tarefas que serão requeridas diversas vezes, dessa forma expondo para o usuário ferramentas padronizadas para a construção, nesse caso, de um servidor *Web*.

#### 4.3.2.1 SANIC

Sanic é um *Web framework* desenvolvido na linguagem Python que expõe API's assíncronas. Seu objetivo é, assim como a linguagem Python, ser simples e eficiente (SANIC, 2018), dessa forma se consolidou em 2018 como o *web framework* mais performático escrito em Python, com potencial de processar mais de 30000 requests por segundo (STACKIFY, 2018).

#### 4.3.2.2 REACT

React é uma biblioteca, escrita em JavaScript, para a construção de interfaces que revolucionou o forma de desenvolver aplicações de visualização, primeiramente por conta da

simples e intuitiva forma de reutilização dos seus componetes, fazendo com que a aplicação final seja coesa, mantendo, assim, um padrão entre as interfaces, e enxuta. Outro motivo da sua dominância no mercado (DIVANTE, 2019) é o JSX, que é uma sintaxe que mistura estruturas consisas de JavaScript e HTML, facilitando o desenvolvimento das telas. Pela simplicidade de implementar aplicações e construir novas telas, e estar em constante desenvolvimento pela comunidade, esse é o Framework que será utilizado para desenvolver a interface do painel de controle.

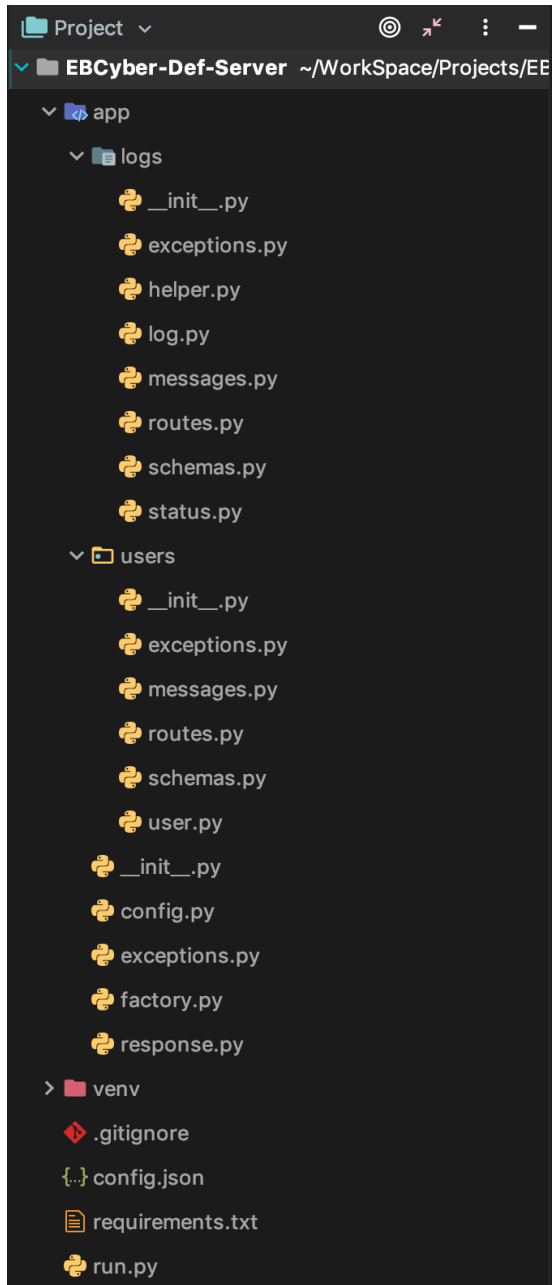
### 4.3.3 BANCO DE DADOS

#### 4.3.3.1 MONGODB

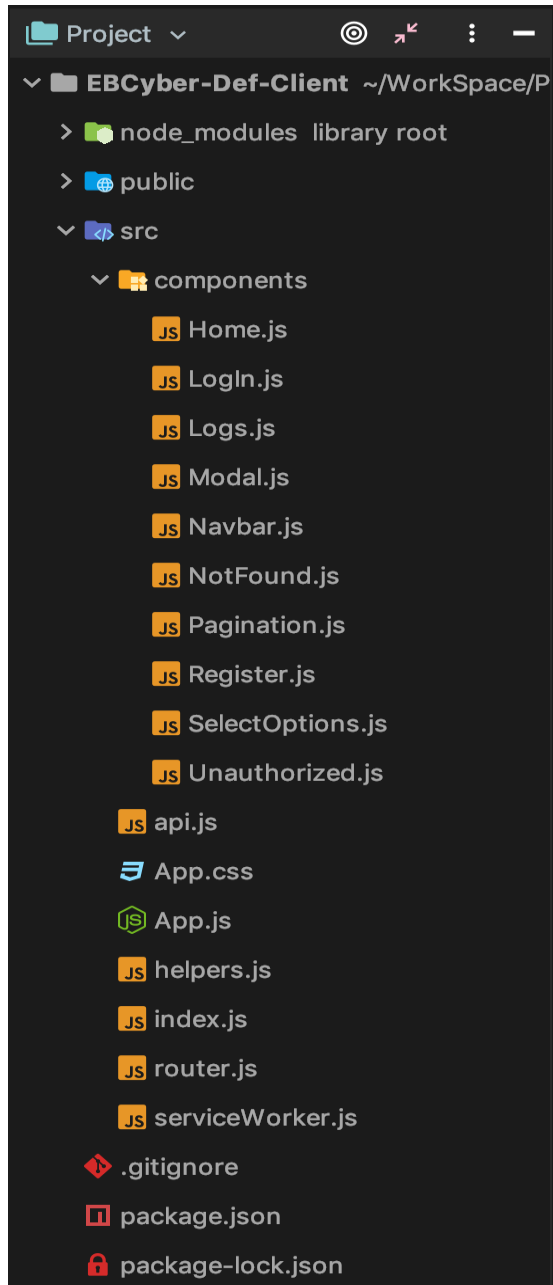
O MongoDB é um banco não relacional que é extremamente flexível e com alta capacidade em escalar, motivos esses que embasaram a escolha desse banco para o projeto. Nele serão armazenados os dados do usuário e as informações sobre os tráfegos de redes suspeitos, definindo, assim, o banco com duas tabelas. A inserção e atualização desses dados será feita exclusivamente pelo servidor, dessa maneira há a garantia de coerência dos dados presentes.

## 4.4 ESTRUTURA

Para desenvolvimento do painel de controle houve a divisão do mesmo em dois subprojetos: EB-CyberDef-Server e EB-CyberDef-Client. A figura 4.1 a seguir demonstra as suas respectivas estruturas.



(a) EB-CyberDef-Server.



(b) EB-CyberDef-Client.

FIG. 4.1: Projetos Servidor e Cliente.

#### 4.4.1 EB-CYBERDEF-SERVER

Escrito em Python e desenvolvido utilizando o Framework Sanic, funciona como o servidor do painel de controle, sendo assim responsável por subir o web server, que irá expor as API's que processarão as requisições advindas do usuário, renderizar o HTML da página principal e ser a única interface com o banco de dados, para assim, manter a consistência de seus dados. A seguir haverá o detalhamento de seus principais módulos e scripts.

##### 4.4.1.1 RUN.PY

É o arquivo principal desse subprojeto. É responsável por fazer as chamadas dos scripts `config.py` e `factory.py` e por rodar o servidor.

##### 4.4.1.2 REQUIREMENTS.TXT

Arquivo de texto que contém todas as dependências de bibliotecas Python do projeto. As dependências para rodar o projeto EB-CyberDef-Server são: `ujson`, é o encoder e decoder de arquivos json escrito em C; `motor`, é o *driver* responsável por fazer a conexão com o banco de dados; `sanic`, é o Web Framework utilizado para subir o servidor do projeto; `aiohttp`, responsável por fazer as chamadas HTTP de forma assíncrona; `passlib`, é uma biblioteca de hashing de senhas para Python 2 e 3 que fornece o gerenciamento dos hashes de senhas existentes; `marshmallow`, responsável por fazer a validação das requisições HTTP recebidas; `python-whois`, provê as informações WHOIS de um determinado domínio; `cached-property`, biblioteca responsável por fazer o cache dos atributos de uma determinada classe de forma simples e eficiente.

##### 4.4.1.3 CONFIG.PY

Carrega o arquivo de configuração do projeto compartilhando, com as API's, dados sensíveis e instanciando o cliente da biblioteca Motor, de forma a realizar a conexão com o banco de dados.

##### 4.4.1.4 FACTORY.PY

Instancia o módulo do servidor do Sanic, definindo suas rotas, tratando possíveis exceções advindas das API's e renderizando o HTML da página de acordo com a interação do usuário. É responsável também por fazer a autenticação, criando uma *hook* que é acionada



antes de toda chamada de API que autentica o valor do *token* recebido na requisição do usuário.

#### 4.4.1.5 LOGS

Esse módulo é reponsável por ser a interface com a tabela de logs no banco de dados, implementando as rotas: `/api/logs/get-log`, `/api/logs/search-logs`, `/api/logs/add-dns-log` e `/api/logs/finish-log`. Além disso define as mensagens que serão retornadas por essas API's e possíveis exceções que possam ocorrer, após a requisição do cliente.

#### 4.4.1.6 USERS

Esse módulo é reponsável por administrar todos os usuários do projeto, criando as rotas de registro, *login* e *logout*, respectivamente definidas pelas REST API's: `/api/users/register`, `/api/users/login` e `/api/users/logout`. Além disso define as mensagens de retorno e trata as exceções relativas à essas API's.

### 4.4.2 EB-CYBERDEF-CLIENT

O subprojeto cliente, por sua vez, foi desenvolvido inteiramente em JavaScript utilizando o Framework React e é a camada de visualização para a presente aplicação. Tem como função, além do interfaciamento direto com o usuário, fazer as chamadas ao servidor, dando continuidade ao pipeline do projeto, e renderizar novos componentes no HTML principal, de acordo com a navegação do usuário pela página.

#### 4.4.2.1 PUBLIC/INDEX.HTML

Por se tratar de uma SPA (single page application), a aplicação possui somente um arquivo HTML, o qual será renderizado pelo servidor. Esse arquivo é responsável por incluir em suas tag *link*, *script* e *body*, respectivamente os arquivos `App.css`, `bundle.js` e `App.js`.

#### 4.4.2.2 BUNDLE.JS

Arquivo gerado após o comando *'build'*, do próprio React, que faz a tradução de forma otimizada de todos os arquivos JavaScript do projeto, que utilizam a sintaxe JSX, para o ECMAScript 6.

#### 4.4.2.3 APP.CSS

Arquivo que contém todos os styles da aplicação, explicitando a descrição de todas as telas do projeto.

#### 4.4.2.4 APP.JS

Componente JavaScript principal da aplicação, o qual definirá, a partir da navegação do usuário, qual componente filho apresentar na interface.

#### 4.4.2.5 COMPONENTS

Este módulo contém todos os componentes JavaScript da aplicação, que são os blocos unitários e reutilizáveis que constroem uma determinada interface no React. Estes componentes estão apresentados na figura 4.1.b.

## 4.5 PROTÓTIPO

### 4.5.1 INTERFACE INICIAL

A página inicial da interface tem como objetivo introduzir ao usuário o projeto EB-CyberDef detalhando o seu objetivo, ilustrando o seu fluxograma e realizando uma breve descrição acerca de cada módulo que o compõe, conforme ilustrado nas figuras 4.2 e 4.3.

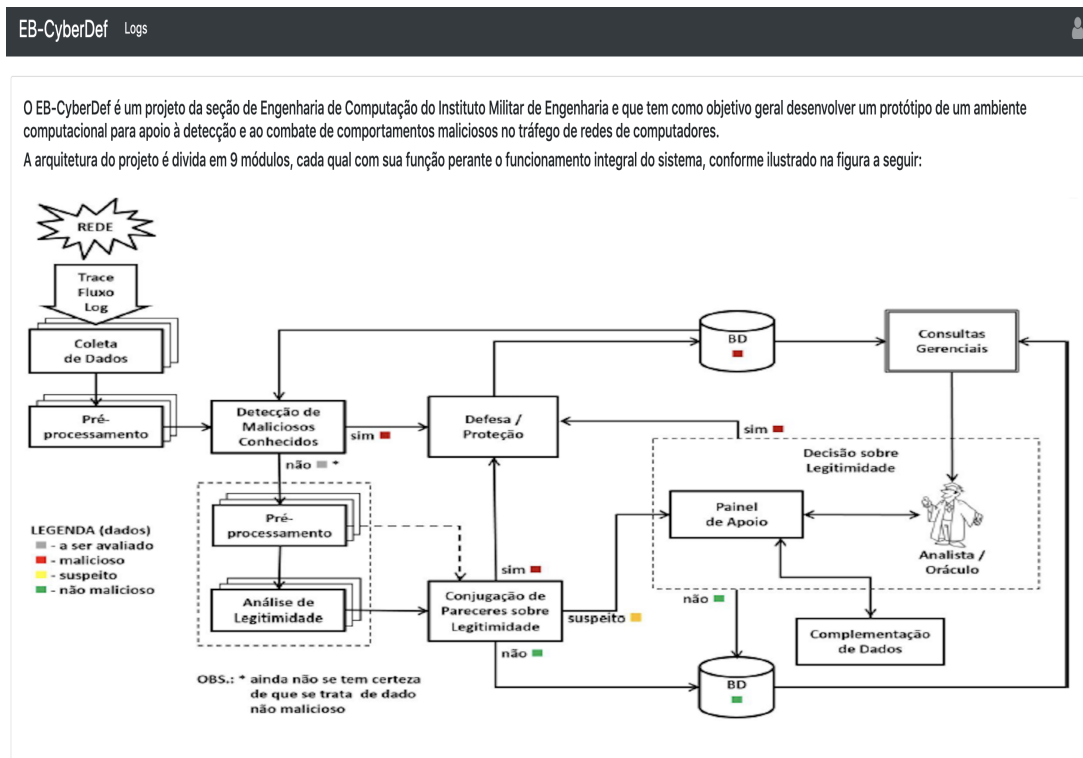


FIG. 4.2: Objetivo e Fluxograma do Projeto Eb-CyberDef.

<p><b>Coleta de Dados</b></p> <p>O módulo de coleta dos dados da rede deve ser capaz de extrair informações de diferentes fontes de dados (traces, logs e fluxos) em vários formatos.</p>
<p><b>Pré-processamento</b></p> <p>Este módulo compreende operações de tratamento e padronização dos dados de redes coletados, de forma a prepará-los para serem processados pelo sistema.</p>
<p><b>Deteção de Maliciosos Conhecidos</b></p> <p>Módulo responsável pela identificação dos dados maliciosos conhecidos (marcados como vermelhos, conforme figura 3.1) através de sua assinatura, isto é, características do código malicioso que podem ser percebidas sem a necessidade de mecanismos baseados em Inteligência Artificial e Aprendizado de Máquina. Este módulo, portanto, utiliza a técnica de deteção baseada em assinatura para realizar uma primeira filtragem dos logs coletados e pré-processados.</p>
<p><b>Defesa/Proteção</b></p> <p>Confirmado que determinado fluxo é malicioso, este módulo deve acionar medidas de defesa e/ou proteção para mitigar o problema. Tais medidas são denominadas Funções de Proteção. Estas funções podem ser especializadas para firewalls, servidores e roteadores. Um exemplo de medida preventiva que pode ser tomada é a adição de uma regra em um firewall com o objetivo de bloquear, exclusivamente, o fluxo malicioso. Conforme Visão Macro-Funcional da arquitetura, exposta na figura 3.1, observa-se que os logs de entrada para este módulo podem ser direcionados a ele em três momentos distintos do processo, após cada uma das etapas responsáveis por decidir se o fluxo é malicioso ou não. Além disso, este módulo é responsável por enviar um registro deste tráfego identificado como malicioso ao banco de dados responsável por manter estes logs (vermelho), de modo que estas informações sejam reutilizadas por outros módulos do sistema.</p>
<p><b>Pré-processamento e Análise de Legitimidade</b></p> <p>Este módulo compreende a execução de algoritmos inteligentes de análise de legitimidade dos dados, responsáveis por avaliar os padrões de dados, procurando classificá-los quanto ao seu potencial em se constituir um padrão malicioso. Ou seja, ele utiliza a técnica de deteção baseada no comportamento da aplicação, tendo como entrada os logs marcados como a ser avaliados (cinza, aqueles que em um primeiro momento não foram identificados como maliciosos, de acordo com a figura 3.1) pelo módulo Deteção de Maliciosos Conhecidos. Cabe ressaltar que a execução dos algoritmos de análise de legitimidade pode ser precedida de diferentes processamentos que irão adequar (pré-processar) os dados conforme a necessidade de cada algoritmo.</p>
<p><b>Conjugação de Pareceres sobre Legitimidade</b></p> <p>Este módulo tem como propósito integrar os pareceres emitidos pelos algoritmos de legitimidade executados pelo módulo anterior, sobre os fluxos que ainda não se tem certeza de que se trata de dado não malicioso, a fim de obter um parecer único que reflita a impressão do sistema quanto à classificação do padrão analisado. Desta forma, o presente módulo deve classificar os dados em (i) certamente não maliciosos (verde), (ii) certamente maliciosos (vermelho) e (iii) suspeito (amarelo). Os dados marcados como verde devem ser enviados a um banco de dados responsável por armazenar tais fluxos não maliciosos. Os dados em vermelho serão enviados ao módulo Defesa/Proteção, abordado anteriormente. A última classificação deve refletir situações em que o sistema não consiga identificar com clareza se o dado é malicioso ou não, sendo este enviado ao módulo de Painel de Apoio.</p>
<p><b>Painel de Apoio</b></p> <p>O módulo de Painel de Apoio tem como objetivo apresentar a um analista humano (oráculo) os resultados da conjugação de pareceres de legitimidade dos fluxos marcados como suspeitos. Diante dos dados apresentados, o oráculo deverá opinar sobre a situação do padrão apresentado e indicar como tal padrão deverá ser tratado pelo sistema. É requisito da interface a ser desenvolvida apresentar também características (destes tráfegos suspeitos) consideradas relevantes ao processo decisório do analista, servindo como um auxílio à sua tomada de decisão. Além disso, caso o oráculo deseje, o painel de apoio poderá apresentar, com o mesmo intuito de ajudar no julgamento, dados externos ao sistema.</p>
<p><b>Complementação de Dados</b></p> <p>Módulo responsável por obter dados externos ao sistema que serão apresentados pelo Painel de Apoio. Conforme seu nome sugere, o módulo de complementação dos dados deve realizar buscas inteligentes cujo resultado possa ser útil para a avaliação do oráculo.</p>
<p><b>Consultas Gerenciais</b></p> <p>Este módulo compreende a exibição de relatórios e consultas gerenciais sobre o comportamento do sistema, permitindo monitorar a qualidade dos resultados encontrados e assim facilitar um eventual ajuste dos parâmetros do sistema a ser realizado na fase de experimentação/configuração.</p>

FIG. 4.3: Detalhamento de cada módulo do Projeto Eb-CyberDef.

## 4.5.2 INTERFACE DE REGISTRO DOS ORÁCULOS

A figura a seguir ilustra o formulário que deve ser preenchido para o registro de um novo oráculo.

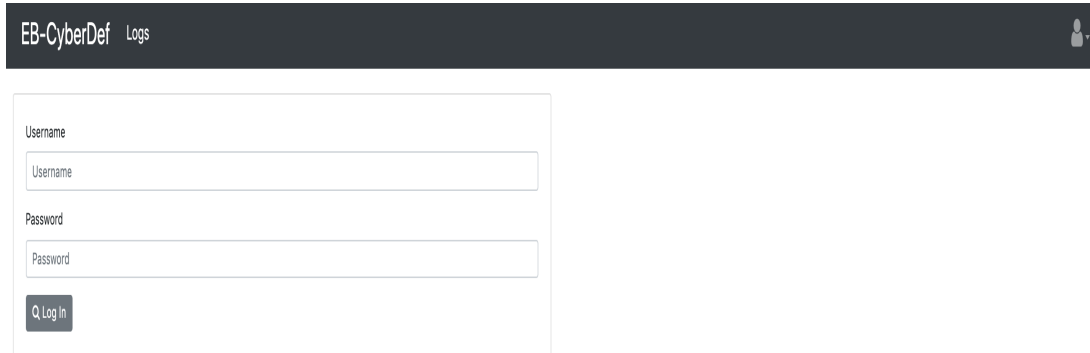
The image shows a web interface for 'EB-CyberDef' with a 'Logs' header. Below the header is a login form with the following fields and a button:

- Username:** A text input field with a placeholder 'Username'.
- Email:** A text input field with a placeholder 'Enter email'.
- Password:** A text input field with a placeholder 'Password'.
- Token:** A text input field with a placeholder 'Token'.
- Log In:** A button with a magnifying glass icon and the text 'Log In'.

FIG. 4.4: Interface de Registro dos Oráculos.

### 4.5.3 INTERFACE DE LOGIN

A tela que o usuário utilizará para se autenticar no sistema é representada pela figura 4.5. A autenticação do usuário é requerida tanto para acesso aos fluxos de rede quanto para decidir sobre a legitimidade dos mesmos.

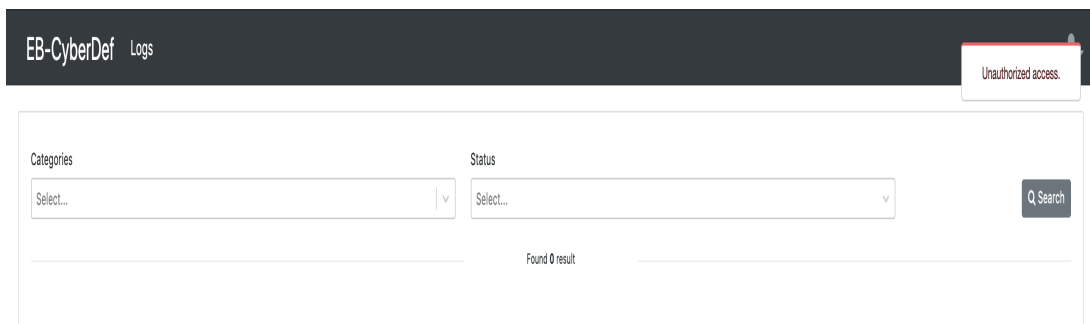


The screenshot shows the login interface for EB-CyberDef Logs. At the top, there is a dark header with the text "EB-CyberDef Logs" and a user icon. Below the header is a white form containing two input fields: "Username" and "Password". Below the password field is a "Log In" button with a magnifying glass icon.

FIG. 4.5: Interface de Login.

### 4.5.4 LISTAGEM DOS TRÁFEGOS DE REDE

A figura 4.6 ilustra a mensagem de acesso não autorizado aos usuário que desejam visualizar os logs, porém não estão devidamente autenticados. Já a figura 4.7 representa a situação de sucesso na listagem dos fluxos de rede.



The screenshot shows the EB-CyberDef Logs interface with an "Unauthorized access." message in a red box at the top right. The main content area contains two dropdown menus labeled "Categories" and "Status", both with "Select..." as the current selection. To the right of these menus is a "Search" button with a magnifying glass icon. Below the search area, it says "Found 0 result".

FIG. 4.6: Acesso não autorizado ao listar os tráfegos de rede.

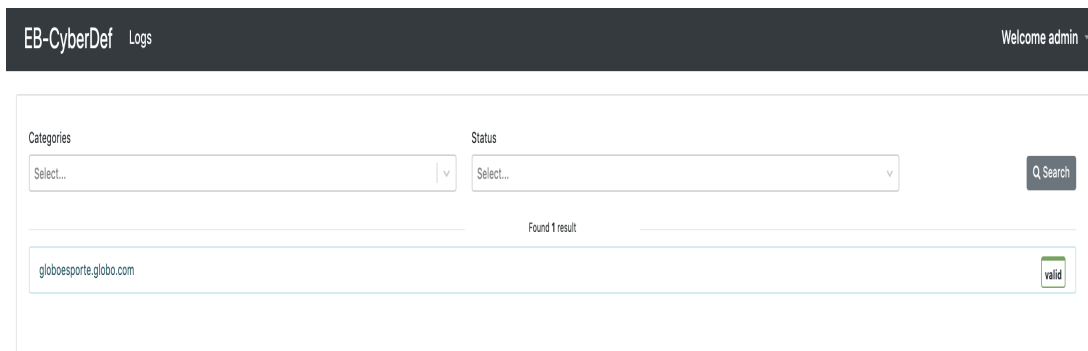


FIG. 4.7: Acesso autorizado ao listar os tráfegos de rede.

#### 4.5.5 INTERFACE DE DETALHAMENTO DO TRÁFEGO DE REDE

Após a listagem dos *logs*, o usuário irá requerir as informações de um fluxo específico, de forma a embasar a sua decisão sobre a legitimidade do mesmo. A figura a seguir ilustra o momento no qual o servidor ainda não respondeu à essa requisição, já a figura 4.9 representa a disposição de todas as *features* relevantes desse log na interface de decisão.

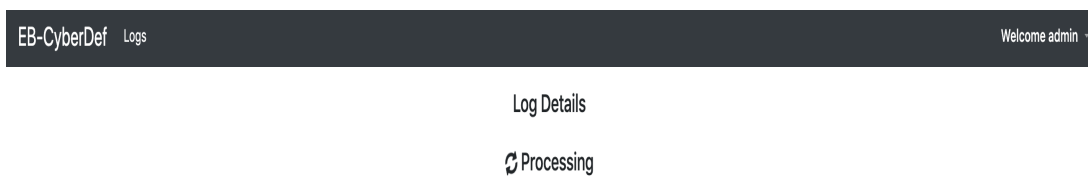


FIG. 4.8: Espera da resposta do servidor com as informações relevantes do *log*

### Log Details

#### General

IP	186.192.81.25	Host Name	globosporte.globo.com	Domain	globo.com
Client IP	127.0.0.1	Client Host	localhost	Client Port	8000
Log Date	2011-07-11T12:00:00.000	Tor	False		

#### HTTP

Response Time	0.064s	URL	https://globosporte.globo.com/	Status	200
Content Type	text/html	Content Length	123666		

#### Location

Country Name	Brazil	Country Code	BRA	City	Jacarepaguá
Continent Name	South America	State Prov	Rio de Janeiro	Zipcode	20000-000
Latitude	-22.96330	Longitude	-43.40480	Top Domain	.br

#### DNS

DNSSEC	unsigned	Type	A	Flags	+
Recursion	Available				

#### Register

Updated Date	2018-05-23T16:27:41Z	Creation Date	1998-12-21T05:00:00Z	Expiry Date	2025-12-21T05:00:00Z
Name	Globo Comunicacao e Participacoes S/A	Street	Rua Lopes Quintas	City	Rio de Janeiro
State/Province	RJ	Country	BR		

#### Admin

Name	Globo Comunicacao e Participacoes S.A.	Street	Av das Americas	City	Rio de Janeiro
State/Province	RJ	Country	BR		



FIG. 4.9: Disponibilização das informações relevantes.

## 5 CONCLUSÃO

Ao considerar o cenário global atualmente, onde os crimes no ciberespaço se reinventam significativamente e são cada vez mais numerosos, possuir uma ferramenta própria e eficiente para a detecção de tráfegos maliciosos é imprescindível para uma instituição com as pretensões do Exército Brasileiro. Assim, baseado na justificativa de desenvolver uma solução própria em segurança cibernética, o projeto EB-CyberDef vem sendo produzido dentro do Instituto Militar de Engenharia, e o desenvolvimento de um dos componentes da sua complexa arquitetura caracterizou-se por ser o principal objetivo do presente trabalho.

Responsável pela criação de um painel de apoio à tomada de decisão do oráculo, o trabalho atingiu de forma satisfatória as metas definidas dentro do escopo estipulado, já que a interface desenvolvida cumpre todos os requisitos e restrições levantadas durante o planejamento do projeto. O painel, além de apresentar adequadamente ao oráculo os fluxos de rede marcados como suspeitos (que chegam do módulo de Conjugação de Pareceres sobre Legitimidade), expõe de forma apropriada as suas características que auxiliam a tomada de decisão do analista.

Em relação a trabalhos futuros, embora a proposta inicial do módulo do Painel de Controle tenha sido concluída com êxito, a evolução do projeto permitiu identificar, em conjunto com os orientadores, diversas oportunidades de aprimoramento até então não percebidas, possibilitando novas implementações em paralelo ao que já foi realizado.

Diversas outras características, além daquelas já levantadas, podem ser exploradas de forma a embasar ainda mais o oráculo a tomar a decisão acerca da legitimidade de um tráfego de rede. Um exemplo destas seria a informação acerca do local de hospedagem do domínio ao que o log se refere. Esta importante informação, cuja ideia de se analisar surgiu apenas na apresentação final do trabalho, proporcionaria uma visão complementar ao conhecimento, também relacionado à geolocalização, já obtido pelo sistema sobre o lugar de registro do domínio. Além disso, devido à divisão do projeto EB-CyberDef em diversos módulos e o desenvolvimento de cada um deles ser feito de forma isolada, outra importante oportunidade para trabalhos futuros refere-se à integração das partes já confeccionadas, de modo que cada subproduto seja incorporado ao ambiente completo do sistema que se deseja criar.



## 6 REFERÊNCIAS BIBLIOGRÁFICAS

- BAILEY, M.; COOKE, E.; JAHANIAN, F.; XU, Y. ; KARIR, M. A survey of botnet technology and defenses.. In: CYBERSECURITY APPLICATIONS TECHNOLOGY CONFERENCE FOR HOMELAND SECURITY, 2009., 2009. **Electronic proceedings...** [S.l.]: IEEE, 2009. Disponível em: <<https://ieeexplore.ieee.org/document/4804459>>. Acesso em: 24 mai. de 2019.
- BISEND. What Is the Difference Between DoS and DDoS Attacks?. Disponível em: <<https://www.bisend.com/blog/difference-between-dos-and-ddos-attack>>. Acesso em: 20 jul. de 2019.
- ZHANHAO CHEN. Newly Registered Domains: Malicious Abuse by Bad Actors. Disponível em: <<https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/>>. Acesso em: 20 aug. de 2019.
- CHUMACHENKO, K. **Machine Learning Methods for Malware Detection and Classification**. 2017. 93 f. Trabalho de Conclusão de Curso (Bacharel em Engenharia) – XAMK - University of Applied Sciences, Finlândia, 2017.
- CISCO. What Are the Most Common Cyberattacks?. Disponível em: <<https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>>. Acesso em: 15 jul. de 2019.
- CISCO. What Is Cybersecurity?. Disponível em: <<https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>>. Acesso em: 15 jul. de 2019.
- CLOUDFLARE. What is a DDoS Botnet?. Disponível em: <<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/>>. Acesso em: 20 jul. de 2019.
- CLOUDFLARE. What is a Denial-of-Service (DoS) Attack?. Disponível em: <<https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/>>. Acesso em: 27 mai. de 2019.

COMODO CYBERSECURITY. WHAT IS A MALWARE ATTACK?. Disponível em: <<https://enterprise.comodo.com/what-is-a-malware-attack.php>>. Acesso em: 27 mai. de 2019.

DEVMEDIA. Introdução às linguagens de programação. Disponível em: <<https://www.devmedia.com.br/introducao-as-linguagens-de-programacao/25111>>. Acesso em: 03 mai. de 2019.

DIVANTE. Top 10 Popular Javascript Frameworks 2019. Disponível em: <<https://divante.co/blog/top-10-popular-javascript-frameworks-2019/>>. Acesso em: 03 mai. de 2019.

DUTRA, A. M. C. Introdução à guerra cibernética: a necessidade de um despertar brasileiro para o assunto. In: SIMPÓSIO DE GUERRA ELETRÔNICA, 9., 2007, São Paulo. **Anais eletrônicos...** Praça Marechal Eduardo Gomes, 50 – Vila das Acácias. CEP 12228-900 – São José dos Campos – SP: Instituto Tecnológico da Aeronáutica, 2007. Disponível em: <<http://www.sige.ita.br/anais/IXSIGE/Artigos/GE39.pdf> > .*Acessoem : 27mai.de2019.*

EB. **EBCyber-Def**. Rio de Janeiro: IME, 2017. 18 p. (Relatório Técnico).

ENISA. What is "Social Engineering"?. Disponível em: <<https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering>>. Acesso em: 27 mai. de 2019.

ENTREPRENEUR. The Growing Menace of Cyber Attacks in the Asia-Pacific region. Disponível em: <<https://www.entrepreneur.com/article/322796>>. Acesso em: 03 mai. de 2019.

EXPLOSION. 5 Most Popular Messaging Apps For 2019. Disponível em: <<https://www.explosion.com/130670/5-most-popular-messaging-apps-for-2019/>>. Acesso em: 27 mai. de 2019.

FASTCOMPANY. 9 things you need to know about the WhatsApp zero-click spyware attack. Disponível em: <<https://www.fastcompany.com/90349568/9-things-you-need-to-know-about-the-whatsapp-spyware-attack>>. Acesso em: 27 mai. de 2019.

FOLHA. Brasil terá mil novos serviços 100% digitais em dois anos, diz secretário. Disponível em: <<https://www1.folha.uol.com.br/tec/2019/02/brasil-tera-mil-novos-servicos-100-digitais-em-dois-anos-diz-secretario.shtml>>. Acesso em: 15 jul. de 2019.

FORBES. The Growing Importance Of Cybersecurity Skills. Disponível em: <<https://www.forbes.com/sites/adigaskell/2018/11/28/the-growing-importance-of-cyber-security-skills/48e32178139d>>. Acesso em: 03 mai. de 2019.

GARCÍA-TEODORO, P.; DÍAZ-VERDEJO, J.; MACIÁ-FERNÁNDEZ, G. ; VÁZ-QUEZ, E. Anomaly-based network intrusion detection: Techniques, systems and challenges.. In: COMPUTERS SECURITY, 28., 2009. **Electronic proceedings...** [S.l.]: Science Direct, 2009, p. 18–28. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0167404808000692>>. Acesso em: 30 mai. de 2019.

WHITE HOUSE. CYBERSECURITY FUNDING. Disponível em: <[https://www.whitehouse.gov/wp-content/uploads/2018/02/ap21\\_cyber\\_security\\_fy2019.pdf](https://www.whitehouse.gov/wp-content/uploads/2018/02/ap21_cyber_security_fy2019.pdf)> .Acessoem : 03mai.de2019.

IMASTERS. O ECMAScript 6 e o futuro do JavaScript. Disponível em: <<https://imasters.com.br/front-end/o-ecmascript-6-e-o-futuro-do-javascript>>. Acesso em: 03 mai. de 2019.

IMPERVA. Distributed denial of service attack (DDoS) definition. Disponível em: <<https://www.imperva.com/learn/application-security/ddos-attacks/>>. Acesso em: 30 jun. de 2019.

INC. The Top 7 Messenger Apps in the World. Disponível em: <<https://www.inc.com/larry-kim/the-top-7-messenger-apps-in-world.html>>. Acesso em: 27 mai. de 2019.

INFOSEC. The Most Common Social Engineering Attacks. Disponível em: <<https://resources.infosecinstitute.com/common-social-engineering-attacks/gref>>. Acesso em: 27 mai. de 2019.

KAIO R. S. BARBOSA, GILBERT B. MARTINS, E. S. E. F. Botnets: Características e métodos de detecção através do tráfego de rede.. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 14., 2014. **Electronic proceedings...** [S.l.]: SBSeg, 2014, p. 99–144. Disponível em: <<http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2014/0036.pdf>>. Acesso em: 27 mai. de 2019.

KHATTAK, S.; RAMAY, N. R.; KHAN, K. R.; SYED, A. A. ; KHAYAM, S. A. A taxonomy of botnet behavior, detection and defense. In: IEEE COMMUNICATIONS SURVEYS

TUTORIALS, 2., 2013. **Electronic proceedings...** [S.l.]: IEEE, 2013, p. 898–924. Disponível em: <<https://ieeexplore.ieee.org/document/6616686>>. Acesso em: 01 mai. de 2019.

LACHOW, I. **Active Cyber Defense - A Framework for Policymakers**. Washington, DC: Center for a New American Security - CNAS, 2013. 13 p. (Relatório Técnico).

MALWAREBYTES. Malware. Disponível em: <<https://www.malwarebytes.com/malware/>>. Acesso em: 27 mai. de 2019.

MARTINS, G. B. **Identificação de Malware Metamórfico baseado em Grafos de Dependência**. 2017. 77 f. Tese (Doutorado em Informática) – Universidade Federal do Amazonas, Amazonas, 2017.

MARZANO, A.; ALEXANDER, D.; FONSECA, O.; FAZZION, E.; HOEPERS, C.; STEDING-JESSEN, K.; ANDITALO CUNHA, M. H. P. C. C.; GUEDES, D. ; JR, W. M. The evolution of bashlite and mirai iot botnets.. In: IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS (ISCC), 2018., 2018. **Electronic proceedings...** [S.l.]: IEEE, 2018, p. 813–818. Disponível em: <<https://homepages.dcc.ufmg.br/cunha/papers/marzano18iscc-botnets.pdf>>. Acesso em: 21 mai. de 2019.

MICHAELIS. ci·ber·es·pa·ço. Disponível em: <<http://michaelis.uol.com.br/busca?r=0f=0t=0palavra=ciberespaço>>. Acesso em: 15 jul. de 2019.

MICHAELIS. vul·ne·ra·bi·li·da·de. Disponível em: <<http://michaelis.uol.com.br/busca?r=0f=0t=0palavra=vulnerabilidade>>. Acesso em: 15 jul. de 2019.

MONTEIRO, S. D. O ciberespaço: o termo, a definição e o conceito. In: DATAGRAMAZERO - REVISTA DE CIÊNCIA DA INFORMAÇÃO, 8., 2007. **Anais eletrônicos...** [S.l.: s.n.], 2007. Disponível em: <<http://www.brapci.inf.br/repositorio/2010/01/pdf31a590c9980007547.pdf>> .*Acessoem : 27mai.de2019.*

NUNES, P. F. V. A definição de uma estratégia nacional de cibersegurança. In: NAÇÃO E DEFESA, 113., 2012, Brasília. **Anais eletrônicos...** [S.l.]: Sociedade Brasileira de Computação, 2012, p. 113–127. Disponível em: <<http://cbsoft2013.unb.br/wp-content/uploads/2013/10/SBES-completo.pdf>>. Acesso em: 21 mai. de 2019.

PHOENIXNAP. 27 Terrifying Ransomware Statistics Facts You Need To Read. Disponível em: <<https://phoenixnap.com/blog/ransomware-statistics-facts>>. Acesso em: 27 mai. de 2019.

PROOF. Ataques de Engenharia Social: tudo que você precisa saber!. Disponível em: <<https://www.proof.com.br/blog/ataques-de-engenharia-social/>>. Acesso em: 27 mai. de 2019.

REID, R.; VAN NIEKERK, J. From information security to cyber security cultures. **2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference**, v. 14, 2014. Disponível em: <<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6950492>>. Acesso em: 29 abr. de 2019.

RIBEIRO, D. S. **UM ESTUDO SOBRE DETECÇÃO E CLASSIFICAÇÃO DE PROCESSOS MALICIOSOS**. 2017. 39 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2017.

SANIC. Documentation. Disponível em: <<https://sanic.readthedocs.io/en/latest/>>. Acesso em: 03 mai. de 2019.

SCHWAB, K. **A Quarta Revolução Industrial**. 1. ed. São Paulo: Edipro, 2016. 160 p.

VOTIRO SECURED. 2018: THE FOUR ZERO DAY ATTACK STATS AND TRENDS YOU NEED TO KNOW. Disponível em: <<https://www.votiro.com/2018-the-four-zero-day-attack-stats-and-trends/>>. Acesso em: 20 jul. de 2019.

ROB SOBERS. Newly Registered Domains: Malicious Abuse by Bad Actors. Disponível em: <<https://www.varonis.com/blog/cybersecurity-statistics/>>. Acesso em: 17 abr. de 2019.

INTERNET SOCIETY. 2018 Cyber Incident & Breach Trends Report. Disponível em: <[https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report\\_2019.pdf](https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf)> .*Acesso em : 20jul.de2019.*

INTERNET SOCIETY. Internet Society. Disponível em: <<https://www.internetsociety.org/>>. Acesso em: 03 mai. de 2019.

STACKIFY. Top 11 Python Frameworks in 2018. Disponível em: <<https://stackify.com/python-frameworks/>>. Acesso em: 03 mai. de 2019.

- STACKOVERFLOW. Most Popular Technologies. Disponível em: <<https://insights.stackoverflow.com/survey/2019/most-popular-technologies>>. Acesso em: 03 mai. de 2019.
- STATISTA. Most popular mobile messaging apps worldwide as of July 2019, based on number of monthly active users (in millions). Disponível em: <<https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>>. Acesso em: 27 jul. de 2019.
- BLACK STRATUS. Your Ultimate Guide to Zero-Day Attacks. Disponível em: <<https://www.blackstratus.com/ultimate-guide-zero-day-attacks/>>. Acesso em: 20 jul. de 2019.
- TABANSKY, L. Basic concepts in cyber warfare. In: MILITARY AND STRATEGIC AFFAIRS, 1., 2011. **Electronic proceedings...** [S.l.: s.n.], 2011. Disponível em: <<http://www.brapci.inf.br/repositorio/2010/01/pdf31a590c9980007547.pdf> > .*Acesso em : 30mai.de2019.*
- TECMUNDO. WannaCry, o ransomware que fez o mundo chorar na sexta-feira (12). Disponível em: <<https://www.tecmundo.com.br/malware/116652-wannacry-ransomware-o-mundo-chorar-sexta-feira-12.htm>>. Acesso em: 27 mai. de 2019.
- SECURITY THROUGH EDUCATION. The Social Engineering Framework. Disponível em: <<https://www.social-engineer.org/framework/influencing-others/pretexting/>>. Acesso em: 27 mai. de 2019.
- PROFISSIONAIS TI. Engenharia Social: as técnicas de ataques mais utilizadas. Disponível em: <<https://www.profissionaisiti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>>. Acesso em: 27 mai. de 2019.
- GTA UFRJ. Botnets. Disponível em: <<https://www.gta.ufrj.br/grad/151/dos/pages/bots.html> > .*Acesso em : 24abr.de2019.*
- VALOR. Segurança cibernética movimentada US\$5,8 bi no Brasil. Disponível em: <<https://www.valor.com.br/empresas/5464667/seguranca-cibernetica-movimentada-us-58-bi-no-brasil>>. Acesso em: 03 mai. de 2019.
- CYBERSECURITY VENTURES. Cybercrime Damages \$6 Trillion By 2021. Disponível em: <<https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>>. Acesso em: 03 mai. de 2019.

CYBERSECURITY VENTURES. Healthcare Security \$65 Billion Market. Disponível em: <<https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/>>. Acesso em: 03 mai. de 2019.

VINCHURKAR, D.; RESHAMWALA, A. A review of intrusion detection system using neural network and machine learning technique. **International Journal of Engineering Science and Innovative Technology (IJESIT)**, v. 1, p. 54–63, 2012.

VORMAYR, G.; ZSEBY, T. ; FABINI, J. Botnet communication patterns.. In: IEEE COMMUNICATIONS SURVEYS TUTORIALS, 19., 2017. **Electronic proceedings...** [S.l.]: IEEE, 2017, p. 2768–2796. Disponível em: <<https://ieeexplore.ieee.org/document/8026031>>. Acesso em: 21 mai. de 2019.

MARKET WATCH. Cyber Security Market 2018 Global Analysis, Segments, Size, Share, Industry Growth and Recent Trends by Forecast to 2023. Disponível em: <<https://www.marketwatch.com/press-release/cyber-security-market-2018-global-analysis-segments-size-share-industry-growth-and-recent-trends-by-forecast-to-2023-2018-10-01>>. Acesso em: 03 mai. de 2019.

WEBROOT. What is Social Engineering?. Disponível em: <<https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering>>. Acesso em: 24 mai. de 2019.

INDUSTRY WEEK. Cyberattacks Skyrocketed in 2018. Are You Ready for 2019?. Disponível em: <<https://www.industryweek.com/technology-and-iiot/cyberattacks-skyrocketed-2018-are-you-ready-2019>>. Acesso em: 03 mai. de 2019.

DIGITAL INFORMATION WORLD. How much time do you spend on social media? Research says 142 minutes per day. Disponível em: <<https://www.digitalinformationworld.com/2019/01/how-much-time-do-people-spend-social-media-infographic.html>>. Acesso em: 15 jul. de 2019.

XU, S.; LU, W. ; LI, H. A stochastic model of active cyber defense dynamics. **Internet Mathematics**, v. 11, p. 23–61, 2015.

ZHU, Z.; LU, G.; CHEN, Y.; FU, Z. J.; ROBERTS, P. ; HAN, K. Botnet research survey. In: IEEE INTERNATIONAL COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE, 32., 2008. **Electronic proceedings...** [S.l.]: IEEE, 2008, p. 967–972. Disponível

em: <<https://ieeexplore.ieee.org/abstract/document/4591703>>. Acesso em: 27 mai. de 2019.