Cybersecurity and the Future of Work in Information Technology

Júlia Marques Boaventura, Phelipe Romano Magalhães Rosa, Rafael Veríssimo, Ryan Marques de Castro, Vinícius Meireles Pereira Santos, Liziane Santos Soares
Instituto de Ciências Exatas e Tecnológicas - Universidade Federal de Viçosa - Campus Rio Paranaíba
Rodovia MG230, Km7, Caixa Postal 22 - 38.810-000 - Rio Paranaíba - MG - Brasil
{julia.m.boaventura, phelipe.rosa, rafael.silva7, ryan.castro, vinicius.m.santos, liziane.soares}@ufv.br

***Abstract*—Cybersecurity is constantly evolving, driven by the growing need for specialized professionals as threats become more sophisticated. With the increasing number of mobile and distributed devices connected to the Internet of Things (IoT), vulnerabilities are more exposed. Advanced Artificial Intelligence models, like Deep Learning, are crucial for detecting ransomware, phishing, and DDoS attacks before they occur. The global shift toward remote and hybrid work, accelerated by the Covid-19 pandemic, has introduced new challenges, including securing home networks and protecting sensitive data outside corporate environments. This article highlights the importance of cybersecurity for the future of IT work, focusing on the current landscape, challenges related to IoT security, the role of Artificial Intelligence in defending against cyberattacks, the rising demand for cybersecurity professionals, and future prospects in the field.**

***Index Terms*—Cybersecurity, Internet of Things (IoT), Artificial Intelligence, Cyberattacks, Cyber Defense, Cybersecurity Workforce.**

I. Introdução

A Era Digital trouxe consigo a popularização de dispositivos e sistemas em nossas vidas, desde pequenos dispositivos para abrir portões até dispositivos portáteis para auxiliar em atividades físicas. Como consequência, há uma crescente dependência tecnológica e da internet no dia a dia, afetando diversas pessoas e serviços básicos. Essa rápida popularização dos dispositivos computacionais, impulsionada pela Internet das Coisas (IoT), resultou na distribuição diária de serviços pelas redes, aumentando a geração e o fluxo de dados sensíveis constantemente. Estima-se que, nos últimos dois anos, 90% dos dados existentes no mundo foram gerados a partir de coletas realizadas por dispositivos como câmeras de monitoramento, sensores, redes sociais e sistemas de e-commerce [1]. Nesse contexto de crescente dependência tecnológica e aumento de dados sensíveis, surgem aqueles que visam tirar proveito dos dados alheios, visualizando, utilizando e até mesmo comercializando o acesso a essas informações. O mau uso desses dados pode acarretar prejuízos que vão além de aspectos financeiros, podendo levar à inviabilização de serviços ou à perda permanente de dados. Pesquisas mostram que setores críticos, como o da saúde, são particularmente vulneráveis a ataques de *ransomware*, que têm crescido exponencialmente [20]. Essas questões levantam o questionamento sobre o futuro da segurança da informação, trazendo o desafio primordial de garantir a integridade e a privacidade desses dados.

Este artigo traz uma visão geral da situação da área de cibersegurança, os avanços tecnológicos, ameaças emergentes, desafios com a IoT na e a demanda por profissionais na área na Seção II. Na Seção III mostramos estudos recentes que exploram abordagens para lidar com ameaças cibernéticas em diferentes dispositivos e contextos. Na Seção IV concluimos trazendo um panorama geral e as dificuldades de implementação 100% eficaz das tecnologias.

II. Estado da Arte em Cibersegurança

Nesta seção abordaremos assuntos relevantes na área de cibersegurança. De início apresentamos ataques cibernéticos comuns e os desafios de segurança relacionados à ambientes e dispositivos IoT. Por último mostramos a utlização de Inteligencia Artificial para proteção de ameaças e a crescente demanda pelos profissionais de cibersegurança.

A. Ataques comuns DDoS, Cavalo de Troia, Ransomware

Não é segredo que, à medida que avançamos tecnologicamente, nosso convívio com a tecnologia também aumenta. No entanto, esse contato vem com possíveis riscos, que podem ser tanto intrapessoais quanto extrapessoais. Nos últimos anos, temos visto um número crescente de organizações, incluindo governamentais, relatando que suas redes foram invadidas ou atacadas por *hackers* [13]. Em geral, esses crimes têm intenções econômicas ou ideológicas [14], sendo lógico que empresas e instituições são os principais alvos desses ataques. Durante o primeiro trimestre de 2023, a média global de ataques semanais aumentou 7% em comparação com o período correspondente em 2022, com cada organização enfrentando uma média de 1.248 ataques por semana [15]. Esse número elevado de ataques cibernéticos tende a crescer à medida que os *hackers* desenvolvem métodos mais criativos de invasão. Um exemplo disso é o ataque DDoS (*Distributed Denial of Service*), que visa tornar serviços e recursos indisponíveis. As consequências podem incluir perdas financeiras, danos à credibilidade, prejuízos à imagem da empresa e problemas com *backups*, armazenamento e serviços em nuvem [14]. Além disso, um fenômeno emergente é o DaaS (*Denial as a Service*), onde a negação de serviço é oferecida como um serviço pago.

Isso aumenta substancialmente a ocorrência de tais ataques, tornando-os um cenário cada vez mais comum.

Outros dois casos recorrentes e de extremo dano são os *malwares* Cavalo de Troia e *Ransomware*. O Cavalo de Troia é um tipo de *malware* que se disfarça como um programa legítimo, enganando os usuários para que o baixem ou o executem. Uma vez ativado, permite ao invasor acesso remoto e controle do computador afetado. Isso possibilita que o invasor monitore em tempo real a atividade ou recupere posteriormente as informações inseridas no sistema comprometido, como senhas, mensagens e dados pessoais [16]. Enquanto o Cavalo de Troia utiliza truques para enganar as vítimas, o *Ransomware* representa uma das formas mais agressivas e sofisticadas de ataque atualmente. É comum "contrair" *ransomware* por meio da rede, links, *downloads* e e-mails. O *ransomware* é projetado para impedir o acesso aos dados pessoais a menos que um resgate seja pago, geralmente em *bitcoin*, o que dificulta o rastreamento [17]. Além da dificuldade de rastreamento, esse tipo de *malware* causa danos em larga escala. Além de infectar o equipamento, o *ransomware* frequentemente busca outros dispositivos conectados, locais ou em rede, e os criptografa [18]. Esse processo de criptografia ocorre de maneira silenciosa, com o *malware* codificando os dados do usuário em segundo plano, sem que o sistema ou *softwares* antivírus possam detectar [18]. O exemplo mais claro desse perigoso ataque é o *Ransomware WannaCry*, que afetou cerca de 200 mil computadores em mais de 150 países, com prejuízos estimados em US$ 1 bilhão [19], sem contar os danos causados pela indisponibilização de serviços essenciais, como os da saúde. Esse tipo de ataque tem crescido globalmente, com um aumento de 105% nos casos de *ransomware* de 2020 para 2021.

Conclui-se a partir disto que os ataques cibernéticos tendem a continuar crescendo, não apenas em frequência, mas também em velocidade, complexidade e alcance. Isso torna o processo de prevenção e mitigação de incidentes cada vez mais difícil e sofisticado [18]. Portanto, é essencial adotar práticas de segurança modernas e promover o conhecimento geral sobre cibersegurança para mitigar os ataques, diminuir as ocorrências e prevenir riscos.

B. Desafios com a IoT

A IoT é uma rede interconectada de dispositivos que se comunicam de forma inteligente, integrando "coisas", isto é, objetos do cotidiano à internet. Isso permite que esses dispositivos troquem informações entre si e com os usuários, oferecendo respostas automáticas e aprimorando a interação entre o ambiente físico e digital [5]. A capacidade de incorporar e integrar esses dispositivos inteligentes está relacionada com a evolução da Internet e da tecnologia sem fio, e está gerando um impacto significativo nas tecnologias da informação e comunicação (TIC) e na Indústria 4.0 [3]. Com toda essa gama de evolução e inovação com os dispositivos em geral, trouxe problemas de segurança relacionados à garantia de confidencialidade, integridade e à não violação das informações trocadas entre os dispositivos IoT. Garantir essa segurança de forma robusta e heterogênea é um grande esforço. Para este caso, soluções tradicionais não são eficazes, e implementações mais robustas são inviáveis por limitações de *hardware*, energia e armazenamento [3].

C. Utilização de Inteligência Artificial para a Proteção contra Ataques

A cibersegurança é um dos pilares fundamentais da era digital. Nas últimas décadas, nos tornamos cada vez mais dependentes da tecnologia e da internet em nossas vidas. Com a digitalização de quase todos os serviços que utilizamos, geramos cada vez mais dados digitais sensíveis que precisam ser protegidos, E as legislações têm exigido, cada vez mais essa proteção e penalizado as plataformas em casos de falhas na segurança dos dados dos usuários [10].

Com o aumento da frequência e da gravidade dos ataques utilizando *softwares* maliciosos, surgiu a necessidade de automatizar a detecção desses *softwares* de forma mais rápida e assertiva [6]. Para isso, o progresso no desenvolvimento de ferramentas de aprendizado de máquina abriu novas oportunidades para utilizá-las na identificação de padrões de ataque, no reconhecimento em tempo real de ataques em andamento e no auxílio na defesa contra essas ameaças.

Esses algoritmos ajudam na identificação de ataques, podendo detectar ameaças aos sistemas antes que a infecção ocorra. Aliados à automatização de respostas, permitem repelir ataques antes mesmo de se concretizarem. Sistemas de Detecção de Intrusão (IDS), por exemplo, monitoram a rede constantemente, permitindo lidar mais rapidamente com um ataque. Ao utilizar a IA como ferramenta na identificação de ameaças, é possível tomar ações imediatas para mitigar danos [6].

No entanto, embora a IA ofereça muitas vantagens, ela também enfrenta desafios, como a necessidade de grandes volumes de dados para treinamento, o risco de falsos positivos ou negativos, ou mesmo a possibilidade de ser enganada por ataques sofisticados. Além disso, cibercriminosos também podem explorar a IA para criar ataques mais avançados e difíceis de serem detectados. Portanto, é fundamental investir no desenvolvimento contínuo e no aprimoramento constante das tecnologias de defesa, garantindo que elas estejam sempre um passo à frente das ameaças emergentes.

D. Crescente demanda por profissionais de cibersegurança

Com o avanço exponencial da conectividade global e o aumento significativo da dependência de tecnologias digitais, o cenário das ameaças cibernéticas se tornou uma preocupação central em todo o mundo. Esse fenômeno impulsionou uma crescente demanda por profissionais especializados em cibersegurança, à medida que governos e empresas reconhecem a cibersegurança como uma prioridade global. Estima-se que o mundo precise de 3,4 milhões de profissionais capacitados para proteger de forma eficaz os ativos digitais. No Brasil, em particular, a necessidade é alarmante, com uma demanda projetada de 312.852 profissionais. Diante desse cenário, a disponibilidade de vagas na área de cibersegurança

supera amplamente a quantidade de profissionais qualificados. Esse descompasso gera uma notável escassez de especialistas, agravada pela alta demanda por vagas e a limitada oferta de mão de obra qualificada. Como consequência, observamos um déficit significativo de profissionais preparados para lidar com os desafios cada vez mais complexos que surgem nesse campo [11]. Os ciberataques estão se tornando mais sofisticados com o passar do tempo, exigindo equipes com habilidades diversas e conhecimentos constantemente atualizados. Essa realidade impõe a necessidade de que os profissionais da área mantenham-se em contínua evolução em termos de tecnologias e métodos de ataque, o que representa um desafio constante para a formação e atualização desses especialistas [7]. Além disso, os criminosos cibernéticos têm explorado variadas formas de coação, muitas das quais lhes proporcionam ganhos substanciais. Um exemplo emblemático é o *Ransomware*, que se estabeleceu como uma das principais ferramentas de extorsão utilizadas por cibercriminosos. Nesse tipo de ataque, os criminosos conseguem acessar, capturar e criptografar os arquivos das vítimas, tornando impossível recuperá-los sem a chave de decriptação, que permanece sob controle dos atacantes. Esse cenário força as empresas a repensarem suas estratégias de segurança, pois a perda ou vazamento de dados de clientes, funcionários e colaboradores pode levar a graves prejuízos financeiros e reputacionais, podendo, em casos extremos, levar à falência da organização [12]. Outro fator que exacerba a demanda por profissionais de cibersegurança é a vigência da Lei Geral de Proteção de Dados (LGPD). A LGPD exige das empresas uma adaptação rigorosa de seus processos, envolvendo a formação de grupos multidisciplinares para o processamento seguro de dados pessoais. No entanto, a implementação da LGPD ainda enfrenta desafios significativos, como o elevado custo associado a sistemas de segurança adequados e a carência de profissionais qualificados. Embora complexa, a intenção da LGPD é clara: tornar o ambiente digital mais seguro e proteger os dados pessoais, prevenindo crimes cibernéticos. Com isso, as organizações enfrentam pressões para garantir a conformidade com requisitos legais cada vez mais rigorosos [10]. A crescente demanda por cibersegurança não se restringe apenas ao aumento das ameaças digitais, mas também reflete as mudanças ocorridas no mundo corporativo durante e após a pandemia de COVID-19. Devido às medidas preventivas adotadas globalmente, muitas empresas se adaptaram ao modelo de trabalho remoto, utilizando plataformas de comunicação de vídeo e aumentando a exposição digital de suas operações. Esse movimento acelerou a transformação digital e a adoção de soluções tecnológicas mais avançadas, o que pode ser visualizado na Figura 1, que mostra a adesão crescente de plataformas de comunicação durante esse período.

Pode-se observar que o aumento na adoção de tecnologias digitais seguiu um crescimento quase linear. Analisando o histórico recente e projetando tendências futuras, como ilustrado na Figura 2, podemos estimar a continuação desse crescimento, especialmente no que se refere à necessidade de profissionais de cibersegurança para suportar a infraestrutura digital expandida.

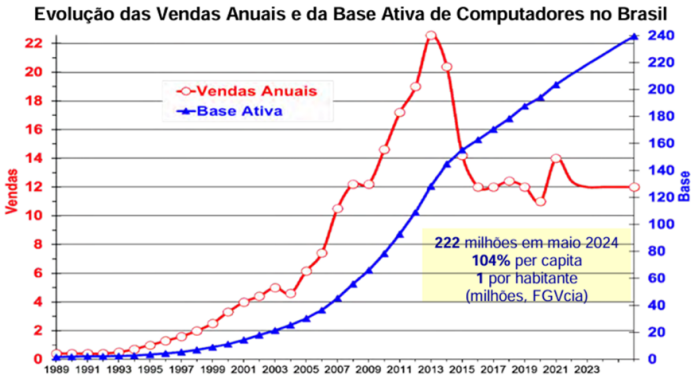


Fig. 1. Evolução das Vendas Anuais e da Base Ativa de Computadores no Brasil [21]

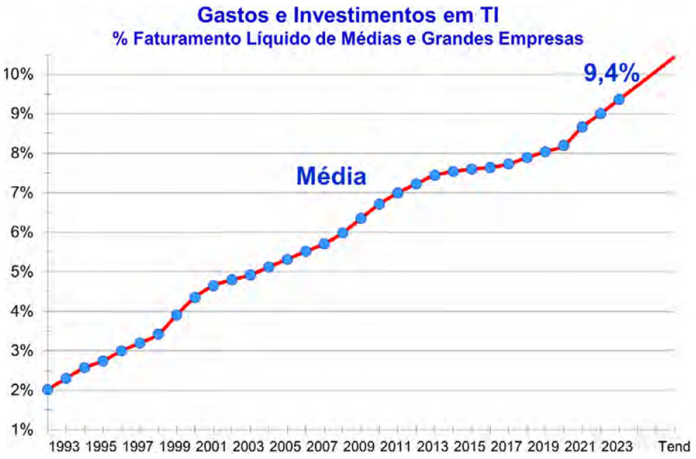


Fig. 2. Média dos Gastos e Investimentos em TI por Médias e Grandes Empresas [21]

Além disso, outro setor que sofreu grande impacto com a transformação digital foi o da saúde. No Brasil, um estudo recente realizado em colaboração com a Associação Nacional de Hospitais Privados (ANAHP) mostrou que 56% dos leitos dos hospitais privados participaram de uma pesquisa específica sobre o uso de TI em hospitais. A evolução dos gastos e investimentos em TI nesses hospitais, comparada à média de outras empresas do setor de saúde, está representada na Figura 3. Observa-se que, embora o percentual de investimentos em TI nos hospitais privados (5%) seja inferior à média geral das empresas (9%), há uma tendência de crescimento que acompanha a evolução do setor de saúde em geral.

Os resultados apresentados indicam que, embora o percentual de investimento em TI nos hospitais privados ainda seja inferior ao da média geral das empresas, a tendência de crescimento é clara, refletindo a importância crescente da tecnologia na área da saúde. Assim, a cibersegurança não se limita apenas a um setor específico, mas torna-se uma

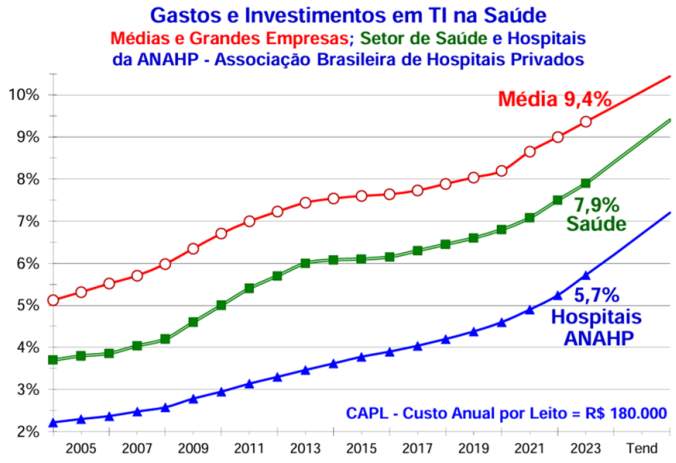


Fig. 3. Gastos e Investimentos em TI por Empresas, Hospitais e Setores Da Saúde [21]

preocupação transversal, afetando diversos setores e exigindo uma maior preparação por parte das empresas e profissionais.

III. Trabalhos Relacionados

Esta seção aborda três estudos relevantes para a área de cibersegurança. Os estudos exploram diferentes abordagens tecnológicas e metodológicas, incluindo um modelo de gestão de riscos em abientes IoT, a aplicação de redes neurais sem peso para detecção de malwares, e a construção de um conunto de dados para análise estática.

A. Um Modelo Declarativo para Gestao de Riscos em IoT

Este trabalho [3] apresenta um novo modelo chamado *Real-Time Risk Management Model* (RTRMM), que utiliza lógica difusa *(Fuzzy Logic)* e probabilidade para gerenciar e mitigá-lós em tempo real, conforme o aprendizado temporal ocorre.

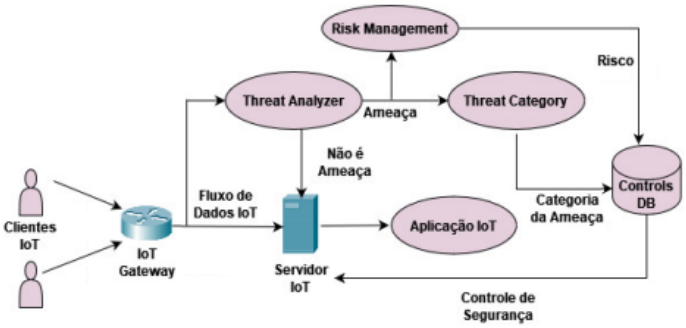
O RTRMM é um modelo para lidar com a segurança em ambientes IoT, utilizando a lógica probabilística para mensurar e mitigar ameaças em tempo real. O principal motivo deste modelo utilizar a lógica probabilística é a possibilidade de lidar com incertezas sobre a existência ou não de ameaças em um ambiente IoT. O seu modelo lógico e estrutura básica, apresentado na Fig 4, descreve um gerenciamento de riscos interativo e contínuo com objetivo de minimizar perdas e maximizar ganhos [3].

O funcionamento do RTRMM é composto por um conjunto de modulos integrados juntamente com o Threat Analyzer que detecta ameças em potencial, em tempo real, que estão nos fluxos de dados de dispositivos IoTs. O *Risk Management* é responsável de receber as ameaças detectadas, analisar e avalia-lás com base em 4 níveis:

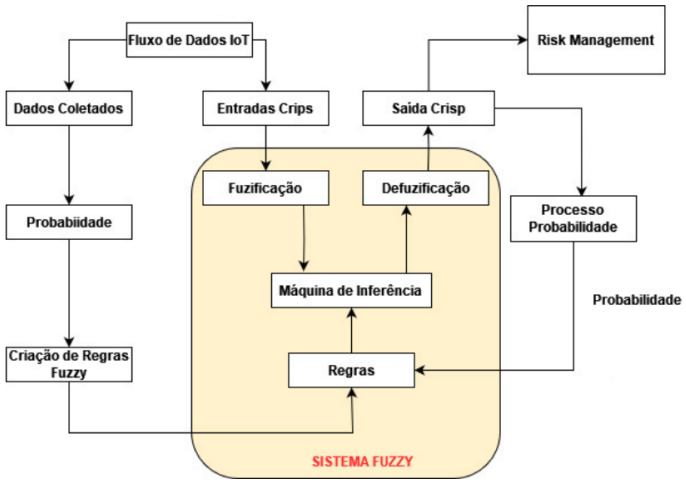
1) *Really*: Grandes chances de ser uma ameaça.
2) *Almost*: Existe uma probabilidade de ser uma ameaça.
3) *Sometimes*: Existe uma probabilidade média de ser uma ameaça.
4) *Impossible*: Poucas chances de ser uma ameaça.

e tomar a decisão de tratar ou não via um processo dinâmico, caso a decisão seja de tratar a ameaça o *Threat Category* estabelece categorias para agilização na seleção de medidas, e a ameaça será enviada ao *Controls DB* onde controles de segurança aplicaram medidas no dispositivo ou ambiente IoT [3]

Abaixo , na Fig 4, temos o modelo lógico e arquitetura do RTRMM e do *Threat Analyzer* respectivamente.



(a) RTRMM



(b) Threat Analyzer

Fig. 4. Modelo Lógico do RTRMM e Arquitetura do Threat Analyzer [3]

O artigo nos mostra um novo modelo para mitigar riscos em ambientes e dispositivos IoT. Nem todos os módulos e funcionalidades foram totalmente implementados ou testados, apenas os módulos de *Threat Analyzer* e *Risk Management* testados e validados, o aprendizado do Threat Analyzer e a escolha da medida a ser aplicada estão em fase de teste e validação. O trabalho teve foco em aplicar o modelo para as medidas que focam no bloqueio de acesso ao dispositivo IoT, a validação completa do modelo ocorrerá em ambientes IoT voltados para a saúde (IoT *Healthcare*) [3].

B. Detecção estática e dinâmica de malwares usando redes neurais sem peso

O trabalho [6], traz uma proposta de utilizar uma rede neural baseada em *RAM Wisard*, da familia de redes neurais sem peso, para detecção estática e dinâmica de *malwares* em

programas. Este tipo de rede neural contém uma diferença das convencionais, ela prioriza a emulação da topologia das conexões usando uma árvore dendrítica e as memórias RAM que guardam as informções representam neurônios artificias, o seu uso pode ser útil se aplicando a grande sistemas computadorizados (sistemas distribuídas, intranets) e ambientes IoT, pelo seu baixo tempo de treinamento e classificação e simplicidade.

Os métodos estáticos trazem uma busca de padrões via opcodes e do arquivo em binário do software, mostrando a distribuição de frequência e fluxo para criar assinaturas que possam ser usadas para identificar cada software. Por ser estática sua aplicação é simples em vista da dinâmica e mostra resultados mais rápidos. Já os métodos dinâmicos, o software é executado em ambiente isolado, de forma a captar padrões de comportamentos por meios da execução de API calls. Por executar em ambiente isolado é mais custosa em tempo e recursos usados [6].

Na Fig 5 é apresentada a arquitetura da rede neural, onde em cada neurônio é realizado um somatório e o maior deles é utilizado.

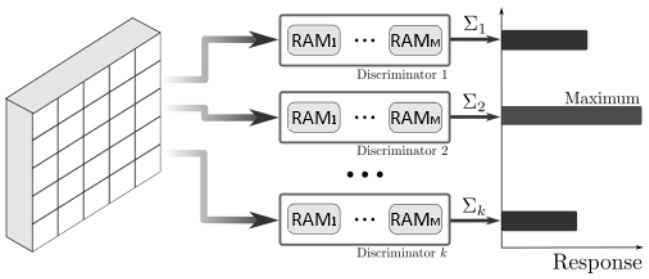


Fig. 5. Arquitetura da Rede Wisard [6]

Este trabalho trouxe como resposta técnologica às ameaças cibernéticas as redes neurias sem peso, focando na *WiSARD*. Foram utilizados conjuntos de dados de imagens convertidas dos programas e de *API calls* para as análises estáticas e dinâmicas. Os experimentos demonstraram uma precisão de 96% na análise estática e 97% na análise dinâmica. O tempo médio da classificação de cada amostra treinada foi abaixo comparado com outros métodos, destacando a *WiSARD* como uma alternativa eficaz na detecção de malwares. Na análise dinâmica, a *WiSARD* obteve tempos de treinamento e classificação de 0,3 milissegundos, mostrando ser eficiente mesmo com uma arquitetura simples, diferente de outros métodos que usam peso [6].

C. Construção de um Conjunto de Dados para Análise Estática de Ransomwares

Neste trabalho, os autores se dedicaram à construção de uma base de dados que futuramente poderá alimentar uma análise estática de *ransomwares*. A construção desse conjunto foi realizada por meio da análise de várias amostras de *malwares* em formato executável, presentes em vários repositórios, especialmente o *VirusShare*[1]. Para confirmar se o vírus é ou não um *ransomware*, foi utilizado o *VirusTotal*[2]. Os autores também extraíram as características desse conjunto escolhido utilizando a biblioteca LIEF[3], que permite analisar, modificar e abstrair arquivos do tipo *Portable Executable* (PE). As características extraídas foram salvas em um arquivo no formato JSON. Por fim, os autores chegaram a uma base de dados final composta por 338 arquivos PE, dentre os quais se destaca o *WannaCry*, que forneceu 57 amostras para o conjunto e que atraiu bastante visibilidade para os ataques de *ransomware*, com vários ataques bem-sucedidos em 2017. O resultado da pesquisa está disponível em um repositório público[4]. Como próximos passos para trabalhos futuros, foram destacados a criação de modelos para a classificação usando aprendizado de máquina e a classificação do *dataset* no modelo [4].

IV. Conclusão e Tendências

A área de cibersegurança está em um crescimento exponencial, tanto no campo da defesa quanto no das ameaças. O Brasil tem uma demanda projetada de 312.852 profissionais para a área, mas ainda é preocupante a necessidade de qualificações adequadas para evitar escassez de especialistas, especialmente considerando que os ataques cibernéticos estão se tornando cada vez mais sofisticados e robustos [11].

Os ambientes e dispositivos IoT estão sendo um desafio para cibersegurança, trazer segurança confiável e eficaz para estes dispositivos é uma tarefa difícil por envolver limitações de *hardware*, como apresentado os trabalhos [3] e [6] utilizaram modelos de probabilidade, lógica difusa e redes neurais respectivamente para mitigar os ricos de ataques em IoT. A tendência da utilização de Inteligência Artificial está cada vez maior, tanto na automação dos processo de defesa contra ataques e de detecção de ataques antes mesmo de acontecerem.

Os algoritmos genéticos enfrentam dificuldades de implementação, desde o treinamento, que exige grandes volumes de dados, até a possibilidade de gerar falsos positivos e/ou negativos, o que pode impactar a segurança de sistemas críticos (ainda que em taxas geralmente muito baixas). Contudo, eles continuam sendo boas opções para identificar ataques em tempo real. Esses algoritmos permitem automatizar a verificação e o tratamento de ataques, algo que seria extremamente difícil de realizar manualmente por seres humanos.

Assim, podemos concluir que a combinação de técnicas tradicionais e abordagens de Inteligência Artificial é essencial para enfrentar os desafios emergentes na cibersegurança. A evolução constante das ameaças requer inovação contínua em estratégias de defesa, bem como capacitação frequente dos profissionais da área, de modo a tentar se colocar sempre um passo à frente dos ataques. Dessa forma, a cibersegurança continuará a se desenvolver como um campo crítico e dinâmico, essencial para a proteção das infraestruturas digitais.

[1]https://virusshare.com
[2]https://www.virustotal.com
[3]https://lief.quarkslab.com
[4]http://gitlab.facom.ufu.br/marcelomborges/ransomware-dataset

REFERENCES

[1] L. F. Borges and M. Nogueira, ”Introdução à Ciência de Dados em Cibersegurança,” Anais Estendidos do XXXVIII Simpósio Brasileiro de Bancos de Dados, SBC, 2023.

[2] E. C. Takeuchi, ”Fatores humanos em cibersegurança: uma revisão sistemática da literatura,” 2023.

[3] L. Lento, P. Patinho, and S. Abreu. ” Um Modelo Declarativo para Gestão de Riscos em IoT”, in Anais do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, Juiz de Fora/MG, 2023, pp. 570-575.

[4] M. Borges, A. Labaki, R. Cattelan, and R. Miani. ” Construção de um Conjunto de Dados para Análise Estática de Ransomwares”, in Anais Estendidos do XVII Simpósio Brasileiro de Sistemas de Informação, On-line, 2021, pp. 41-44.

[5] ”What is IoT”. AWS Amazon.[Online]. Disponível: What is IoT [Acesso em 19-08-2024].

[6] L. Ramos, L. Lusquino Filho, F. França, and P. Lima. ” Detecção estática e dinâmica de malwares usando redes neurais sem peso”, in Anais do XX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, Petrópolis, 2020, pp. 369-381.

[7] ”Cresce demanda por profissionais de cibersegurança no mercado brasileiro”.DatacenterDynamics.[Online]. Disponível: Cresce demanda por profissionais [Acesso em 22-08-2024].

[8] ”Cibersegurança: avanços tecnológicos transformam a defesa digital”. IBSEC. [Online]. Disponível: Avanços tecnológicos [Acesso em 22-08-2024]

[9] ”O que é resposta a incidentes?”. IBM. [Online]. Disponível: ”O que é resposta a incidentes?” [Acesso em 22-08-2024]

[10] B. E. de Melo Cunha et al., ”As dificuldades da implementação da LGPD no Brasil,” Revista Projetos Extensionistas, vol. 1, no. 2, pp. 39-47, 2021.

[11] ”A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution”. (ISC)2. [Online]. Disponível: A critical need for cybersecurity professionals [Acesso em 22-08-2024]

[12] DE OLIVEIRA FORNASIER, Mateus; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. Revista Thesis Juris, v. 9, n. 1, p. 208-236, 2020.

[13] W. M. Junior ”Cibersegurança nas Organizações: a Contratação de Testes De Invasão como Estratégia Competitiva” Must University, 2023.

[14] D. Alves ”Ataques cibernéticos ao Brasil: levantamento sistemático dos últimos dez anos (2010 – 2020)”, Universidade Federal do Rio Grande do Sul. Faculdade de Ciências Econômicas, 2022.

[15] ”Média Global de Ciberataques Semanais Aumentou 7% no Trimestre”. Security Leaders.[Online]. Disponivel: ”Média Global de Ciberataques Semanais Aumentou 7% no Trimestre” [Acesso em 27-08-2024].

[16] M. C. N. Carvalho ”O Malware Enquanto Meio de Obtenção de Prova”, Universidade Lúsiada. 2024.

[17] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, M. K. Khan ”Ransomware: Recent advances, analysis, challenges and future research directions”, Canadian Institute for Cybersecurity, University of New Brunswick, Center of Excellence in Information Assurance, University, Riyadh 11653, Saudi Arabia. 2021.

[18] E. P. Riccetto, S. Santos ”Ransomware: Sua Evolução Histórica e Como Funciona na Prática”, Americana-SP. 2022.

[19] S. V. N. Silva, I. G. Junior ”Ransomware: A Evolução Dos Ataques Na Contemporaneidade e Seus Desafios para a Segurança Digital”, Journal of Technology & Information. 2023.

[20] ”Setor da saúde é o terceiro mais atacado em 2024 pelo cibercrime no Brasil”. Kaspersky.[Online]. Disponivel: ”Setor da saúde é o terceiro mais atacado em 2024 pelo cibercrime no Brasil” [Acesso em 27-08-2024].

[21] ”35ª Pesquisa anual do FGVCIA: Uso da TI nas empresas. Disponivel: ”35ª PESQUISA ANUAL DO FGVCIA: USO DA TI NAS EMPRESAS” [Acesso em 23-08-2024].