Extração e Análise de Indicadores de Comprometimento (IoCs) em Fóruns da *Dark Web*

Sebastião Alves de Jesus Filho[1], **Paulo Henrique Ribeiro Gabriel**[1], **Rodrigo Sanches Miani**[1]

[1]Faculdade de Computação - FACOM – Universidade Federal de Uberlândia (UFU)
Av. João Naves de Ávila, nº 2121, Santa Mônica, Uberlândia – MG – Brasil

{sebastiao,phrg,miani}@ufu.br

Abstract. *With the increase and sophistication of attacks on information systems, it becomes essential to extract cyber threat intelligence. In this regard, Indicators of Compromise (IoCs), which consist of signals capable of identifying malicious activities in computer systems, deserve attention. This work is dedicated to the extraction and analysis of IoCs in Dark Web forums, aiming to provide relevant information for information security. The results indicate an incidence of IoCs above 26%, with the majority being URLs. Furthermore, it was found that posts in computer-related categories have almost twice the number of IoCs compared to other categories.*

Resumo. *Com o aumento e sofisticação dos ataques aos sistemas de informação, torna-se essencial extrair inteligência de ameaças cibernéticas. Nesse sentido, os Indicadores de Comprometimento (IoCs), que consistem em sinais capazes de identificar atividades maliciosas em sistemas computacionais, merecem atenção. O presente trabalho dedica-se à extração e análise de IoCs em fóruns da Dark Web, com o objetivo de fornecer informações relevantes à segurança da informação. Os resultados encontrados indicam uma incidência de IoCs superior a 26%, sendo a maioria URLs. Além disso, constatou-se que os posts das categorias relacionadas à computação possuem quase o dobro de IoCs em comparação com outras categorias.*

1. Introdução

Os avanços tecnológicos impulsionam a crescente conectividade global. Atividades como trabalho, lazer, educação, compras e transações financeiras têm impelido a necessidade de dispositivos computacionais interconectados em rede. No entanto, a crescente visibilidade online também traz consigo um aumento nos riscos de ataques cibernéticos, que frequentemente resultam em consequências adversas significativas para indivíduos e entidades.

Nos últimos anos, houve um aumento significativo de ações ilícitas na Internet como roubo de dados financeiros, extorsão e espionagem cibernética [Brooks 2021]. Recentemente, empresas como Lojas Renner, JBS e *Colonial Pipeline* foram alvo de ataques de *ransomware*. Ao mesmo tempo, ocorreram diversos vazamentos de senhas, como o caso da empresa *RockYou* [Cubrilovic 2018], e o vazamento de dados pessoais de cidadãos brasileiros [Olhar Digital 2021], o que ilustra o impacto financeiro e social dos ciberataques. Nesse contexto, a *Dark Web*, reconhecida por preservar o anonimato, torna-se um ambiente propício para o compartilhamento de informações entre cibercriminosos.

De acordo com [Sapienza et al. 2017], agentes maliciosos seguem uma série de etapas para conduzir ataques cibernéticos. Esses passos incluem a identificação de vulnerabilidades, a aquisição de ferramentas e habilidades, a seleção do alvo, a criação ou obtenção de infraestrutura, e o planejamento e a execução do ataque. Durante essas fases, os agentes maliciosos podem deixar rastros associados a atividades específicas, como tentativas de acesso a URLs incomuns ou a manipulação de listas de e-mails corporativos. Esses vestígios são conhecidos como Indicadores de Comprometimento (IoCs) [Jo et al. 2022], funcionando como uma espécie de impressão digital que pode ser observada por especialistas em segurança da informação. Além disso, exemplos adicionais de IoCs compreendem endereços *Internet Protocol* (IP), nomes de domínio e *hashes* de arquivos.

O termo Indicadores de Comprometimento (IoCs) está diretamente ligado a Inteligência de Ameaças Cibernéticas, do inglês *Cyber Threat Intelligence* (CTI), que, de acordo com [Zhang et al. 2019], consiste em um conhecimento baseado em provas que analisa e explica os pormenores das ameaças de segurança cibernética existentes ou em evolução. Uma forma de compartilhar CTI é através dos IoCs. Tendo em vista o crescente número de ameaças cibernéticas, o compartilhamento de informações de inteligência que visam mitigar os riscos de comprometimento da informação é fundamental para a comunidade de segurança cibernética. [Basheer and Alkhatib 2021] também destacam a importância da análise de conteúdo em plataformas *Dark Web* para detectar e prever crimes cibernéticos. Esses fatores reforçam a importância do desenvolvimento de ferramentas para extração e análise de IoCs.

Nos últimos anos, diversos estudos têm se concentrado na identificação de ameaças de segurança a partir da análise de conteúdo presente em fóruns da *Dark Web* [Sapienza et al. 2017], [Dong et al. 2018] e [Sarkar et al. 2019]. Com relação à análise e extração de IoCs, [Niakanlahiji et al. 2019] investigam a existência de IoCs no *Twitter*, enquanto que [Zhang et al. 2019] extraem IoCs realizando buscas na *Surface Web*, usando como entrada indicadores como domínios e endereços IP que tenham sido considerados suspeitos de acordo com informações de ameaças de código aberto. Por sua vez, [Caballero et al. 2023] direcionam seus esforços para extrair IoCs de seis diferentes fontes: *Blogs RSS, Twitter e Telegram*, bem como *Malpedia, APTnotes* e *ChainSmith*, que são repositórios de projetos relacionados à segurança cibernética. No entanto, nenhuma dessas investigações sobre IoCs foram conduzidas na *Dark Web*.

Portanto, o presente trabalho discute a relação de IoCs com fóruns da *Dark Web*, tendo como foco a busca, extração e análise desses indicadores em dados coletados nesses fóruns de discussão, visando responder às seguintes questões de pesquisa:

1. Qual é a incidência de IoCs em fóruns da *Dark Web*?
2. Quais são os tipos mais frequentes de IoCs encontrados nos *posts* desses fóruns?
3. Existe algum fator que influencia a incidência de IoCs nos *posts* desses fóruns?

Foram coletados 26.994 *posts* em dois fóruns da *Dark Web*: o *Hidden Answers* e o *Deep Answer*. Destes, foram extraídos dez tipos de IoCs: *URL, E-mail, Domínio, Hash, IPv4, IPv6, ASN, CVE, MAC e Registry Key Path*. Cinco desses tipos foram extraídos utilizando uma ferramenta desenvolvida pelos autores, enquanto os outros cinco foram obtidos por meio da ferramenta *ioc-finder*, desenvolvida por Forrest Hightower [Hightower 2017]. Espera-se que os resultados encontrados no trabalho possam melho-

rar a compreensão acerca do uso da *Dark Web* como fonte de dados para CTI, além de fornecer insumos para o desenvolvimento de aplicações como a caracterização de *posts* maliciosos.

O restante do artigo está organizado da seguinte forma: Na Seção 2, são apresentados trabalhos relevantes que contribuíram para o desenvolvimento desta pesquisa. A Seção 3 apresenta conceitos fundamentais sobre IoCs, *Deep Web* e *Dark Web*. A Seção 4 detalha cada etapa do desenvolvimento do estudo. Os resultados obtidos são discutidos na Seção 5, e as conclusões do artigo são apresentadas na Seção 6.

2. Trabalhos Relacionados

A literatura atual apresenta estudos que utilizam dados coletados em redes sociais e fóruns da *Dark Web* para identificar postagens maliciosas e prever incidentes de segurança. Esses estudos partem do pressuposto de que é possível identificar sinais de um ataque cibernético nessas fontes antes que ele seja executado. Outros estudos se concentram no compartilhamento de CTI, usando extração de IoCs em redes sociais, como o *Twitter*, *Telegram* e até mesmo na *Surface Web*. A seguir, serão descritos alguns desses estudos.

[Sapienza et al. 2017] propuseram uma estrutura que aproveita sensores de mídia social, em especial *Twitter* e fóruns da *Dark Web*, para gerar alertas antecipados de ameaças cibernéticas. Os autores usaram como estratégia, o monitoramento de contas no *Twitter* de especialistas, pesquisadores e *hackers* éticos escolhidos manualmente, a fim de encontrar postagens de exploração de vulnerabilidades. Usando técnicas de mineração de texto, selecionam termos importantes e removem os irrelevantes, tendo como base dicionários pré-definidos. Em seguida, verifica se os termos descobertos também já foram mencionados em fóruns de *hackers* da *Dark Web* previamente selecionados. Durante o período observado, 84% dos avisos gerados foram considerados relevantes por especialistas.

[Dong et al. 2018] utilizaram um método parecido com a estrutura proposta por [Sapienza et al. 2017]. Porém aqui, a coleta de dados é feita apenas em fóruns da *Dark Web*. O principal objetivo é a descoberta de novas ameaças cibernéticas. A ideia consiste em monitorar alguns dos maiores mercados da *Dark Web* a fim de coletar itens relacionados a segurança cibernética. Em seguida, os itens são classificados em quatro categorias *(1–data, 2-carding, 3-hack, 4-others)*. O foco do sistema é na categoria *3-hack*, que inclui (vulnerabilidades, ferramentas de *hacking, malwares*, tutoriais de exploração, etc). Com o uso de técnicas de mineração de texto, caracteres especiais e palavras irrelevantes são removidas, ficando apenas os termos que consideram ser importantes. Dentre esses termos, os que ainda não são conhecidos pelo sistema podem significar o surgimento de novas vulnerabilidades ou *malwares*. O próximo passo é verificar se o termo descoberto se trata de uma nova ameaça ou se refere a uma já existente. Por fim, o sistema gera avisos para os termos recém-descobertos. Os resultados dos testes na etapa de classificação tiveram boa precisão, atingindo 94%.

Já [Sarkar et al. 2019] usaram informações de fóruns da *Dark Web* aproveitando a estrutura de rede de respostas das interações do usuário com o objetivo de prever ataques cibernéticos corporativos. O sistema tenta prever se haverá um ataque cibernético em um determinado dia para uma organização, para isso aplica modelos de aprendizado supervisionado em um conjunto de recursos extraído dos fóruns. Os resultados apresen-

tados mostraram que o sistema teve uma boa precisão e foi capaz de prever importantes incidentes de segurança que ocorreram no período de testes.

[Niakanlahiji et al. 2019] apresentaram um *framework* escalável para extração automática IoCs do *Twitter*, utilizando uma combinação de teoria dos grafos, aprendizado de máquina e técnica de mineração de texto. O sistema conta com um modelo de reputação para descobrir perfis confiáveis que publicam informações de CTI e apenas rastreia o fluxo de *tweets* desses perfis. Os autores relataram que, ao longo de quatro semanas, o sistema identificou mais de 1.200 IoCs, incluindo URLs maliciosas."

Já [Zhang et al. 2019] apresentaram um sistema capaz de extrair automaticamente IoCs da *Surface Web*, verificando indicadores suspeitos com a ajuda de informações de ameaças de código aberto. O sistema recebe como entrada indicadores considerados suspeitos, como domínios e endereços IP, e verifica se são de ameaças reais, coletando e analisando ativamente suas informações relevantes sobre ameaças de código aberto na *Surface Web*. Com base nos resultados da verificação, o sistema gera uma lista de IoCs. Em seguida, extrai automaticamente novos indicadores das páginas da web relacionadas aos IoCs como novas entradas, repetindo o processo de verificação para gerar mais IoCs.

No trabalho [Al-Ramahi et al. 2020], foi apresentada uma abordagem sistemática para extrair automaticamente Tópicos de Interesse (ToIs) de sites de *hackers*, visando utilizá-los como entradas para controles de segurança acionáveis ou coletores de IoCs. Em um primeiro momento, os autores analisaram postagens de *hackers* em um conjunto de dados público. Como segundo experimento, desenvolveram um rastreador para extrair ToIs em um fórum da *Dark Web*. Os resultados foram positivos, porém os autores relataram vários desafios relacionados ao rastreamento e extração de ToIs relevantes.

[Caballero et al. 2023], apresentaram uma plataforma para extrair IoCs de seis diferentes fontes: *Blogs RSS, Twitter e Telegram*, bem como *Malpedia, APTnotes* e *ChainSmith*, que são repositórios de projetos relacionados à segurança cibernética. Além de terem desenvolvido a ferramenta de extração de IoCs, os autores relataram que fizeram uma análise para avaliar a precisão de outras 7 ferramentas de extração de IoCs. Os resultados mostraram que a ferramenta desenvolvida obteve maior precisão em 11 dos 13 tipos de IoCs extraídos.

Os trabalhos relatados trouxeram importantes contribuições na identificação de incidentes de segurança e extração de IoCs. No entanto, é importante ressaltar que nenhum desses estudos teve o foco voltado especificamente para a extração e análise empírica de IoCs em fóruns da *Dark Web*. Essa lacuna na pesquisa motivou o presente estudo, que se propõe a preencher essa falta de investigação ao desenvolver métodos e técnicas específicas para a extração e análise de IoCs em fóruns da *Dark Web*. Dessa forma, espera-se que os resultados deste estudo contribuam para o avanço do conhecimento nessa área e forneçam *insights* valiosos para a detecção e prevenção de ameaças cibernéticas.

3. Fundamentação Teórica

Nesta seção, são abordados os conceitos de IoCs (Subseção 3.1) e *Deep Web* e *Dark Web* (Subseção 3.2). A compreensão desses conceitos é essencial para a análise de ameaças e ações maliciosas na Internet, além de ser fundamental para o desenvolvimento de estratégias de segurança eficazes.

3.1. Indicadores de Comprometimento (IoCs)

Os Indicadores de Comprometimento (IoCs) são elementos importantes para detectar e identificar atividades maliciosas em sistemas de informação. Eles consistem em sinais específicos, tais como endereços IP, nomes de domínio, URLs e *hashes* de arquivos, que auxiliam os analistas de segurança a determinar se um sistema foi comprometido.

[Niakanlahiji et al. 2019] destaca que os IoCs podem ser classificados de diferentes maneiras, sendo a mais comum aquela que se baseia na granularidade dos dados representados pelos IoCs. Nesta classificação, os IoCS são divididos em três grupos: IoCs atômicos, computados e comportamentais. Exemplos de IoCs atômicos são: endereços IP, nomes de domínio e chaves de registro. Já os IoCs computados são aqueles calculados a partir de dados observados durante um ataque, como por exemplo valores de *hash* de instâncias de *malware*. Por fim, os IoCs comportamentais são uma combinação dos dois outros tipos.

Para [Asiri et al. 2023], além de estar ciente dos agentes de ameaças e tipos de ataques, as equipes de segurança precisam também conhecer os dados associados a esses ataques cibernéticos, chamados de IoCs. Esse conhecimento pode melhorar o tempo de resposta a um incidente de segurança. Por outro lado, segundo [Jo et al. 2022] os IoCs são apenas um dos tipos de dados CTI e não devem ser o único foco das estratégias de segurança cibernética, já que as ameaças estão em constante evolução e se tornando cada vez mais sofisticadas.

3.2. *Deep Web* e *Dark Web*

Os termos *Deep Web* e *Dark Web* são muitas vezes tratados como sinônimos, no entanto existe diferença entre os dois. Primeiramente é importante lembrar que o termo *Web* é usado para definir a parte da Internet que é acessível por meio de mecanismos de busca convencionais, como *Google, Yahoo e Bing*. Por esse motivo, é chamada de *Surface Web*. Por outro lado, na *Deep Web* hospeda-se conteúdo protegido por senha, como contas bancárias *online*, serviços de e-mail privados entre outros. Finalmente, a *Dark Web* é uma parte oculta e obscura da *Deep Web* que é acessível apenas através de ferramentas de navegação anônimas.

Para [Bradbury 2014], o conceito de *Deep Web* e *Dark Web* refere-se a duas entidades distintas. A *Deep Web* consiste em páginas da Web que são acessíveis na Internet pública, porém não podem ser encontradas por meio de mecanismos de pesquisa convencionais, como o *Google*. Por outro lado, a *Dark Web* representa uma parte da Internet que geralmente é acessível publicamente, mas requer conhecimento específico para encontrá-la, pois está situada em uma camada alternativa da Internet onde o anonimato é valorizado. Ainda segundo [Bradbury 2014], a *Dark Web* tem sido associada a atividades criminosas, como venda de armas e drogas, redes de *hackers* e lavagem de dinheiro. No entanto, também é utilizada por pessoas que buscam contornar medidas de censura impostas por regimes não democráticos.

[Basheer and Alkhatib 2021] destaca que a *Deep Web* é a parte da *Web* que os motores de busca não podem acessar por diferentes razões relacionadas às funções operacionais dos sites. Estima-se que essa parte representa mais de 90% de toda a Internet. A *Dark Web* faz parte da *Deep Web*, nela técnicas de criptografia especial são usadas para ocultar as identidades e endereços IP dos usuários. [Saleem et al. 2022] reforçam

que a rede oculta e o anonimato da *Dark Web* abrem caminho para atividades ilegais e colaboram com os cibercriminosos na execução de ciberataques.

3.2.1. Fórum da *Dark Web*

Um fórum da *Dark Web* é uma plataforma online onde os usuários podem discutir sobre vários tópicos. Geralmente um fórum é dividido em categorias, sendo cada uma dedicada a um tema específico, como *hacking*, drogas, dinheiro e mercados. No entanto, de acordo com [Al-Ramahi et al. 2020], os usuários nem sempre seguem essas categorias predefinidas e podem postar conteúdo relacionado a um tópico específico em uma categoria diferente. [Akhgar et al. 2021], enfatizam que para acessar um fórum na *Dark Web*, os usuários precisam usar navegadores especializados, como o *Tor (The Onion Router)*, que roteia o tráfego da Internet através de vários servidores em todo o mundo, tornando difícil rastrear a identidade do usuário.

Para inserir conteúdo em um fórum na *Dark Web*, o usuário segue alguns passos básicos: escolhe uma categoria, define um título e, em um campo separado, pode detalhar o conteúdo de sua postagem. Tanto no título quanto no conteúdo, é comum compartilhar informações ou fazer perguntas. A postagem inicial pode receber respostas e comentários de outros usuários, o que é conhecido como interações e depende da relevância do conteúdo. Embora qualquer resposta, comentário ou mensagem inicial possa ser considerado um *post*, neste trabalho um *post* é definido como um conjunto de mensagens relacionadas a um tópico específico. O número de interações e se elas ocorreram não afetam a definição de um *post*.

4. Desenvolvimento

Nesta seção, é apresentada a metodologia empregada, com o objetivo de descrever as etapas desenvolvidas até a conclusão do trabalho. A Figura 1 ilustra a estrutura geral da solução implementada, que é composta por três etapas principais (I, II e III). Cada uma dessas etapas será descrita em detalhes nas Subseções 4.1, 4.2 e 4.3, respectivamente.

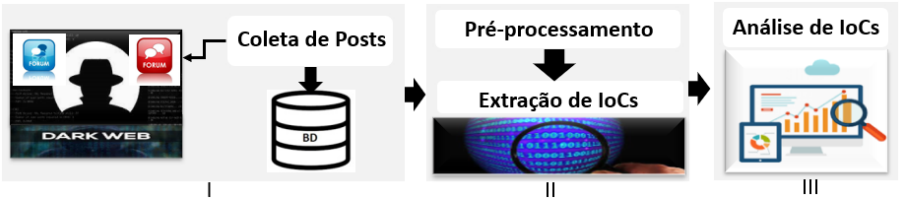

Figura 1. Etapas do desenvolvimento da pesquisa

4.1. Etapa I - Coleta de *Posts*

A primeira etapa do processo consiste na coleta de *posts* de dois fóruns da *Dark Web*: o *Hidden Answers* e o *Deep Answer*. Esses fóruns foram escolhidos por serem considerados abertos, ou seja, acessíveis a qualquer usuário que tenha o *link* ou a URL correspondente. Ao contrário de fóruns restritos ou privados, que exigem convites ou senhas para permitir o acesso, os fóruns abertos são mais acessíveis e costumam ter um fluxo maior de informações e atividades. Para realizar essa coleta, foi utilizado um *crawler* – um sistema automatizado que varre os fóruns em busca de postagens. Os dados coletados são, então, armazenados em uma base de dados para análise posterior.

4.2. Etapa II - Pré-processamento e Extração de IoCs

Na segunda etapa do processo, foram desenvolvidos dois módulos inter-relacionados: o módulo de pré-processamento dos dados coletados e o de extração de IoCs. O objetivo do pré-processamento foi limpar e organizar os dados, o que envolve tarefas como a exclusão de colunas desnecessárias para a análise, a padronização dos nomes das colunas dos fóruns, a junção dos *posts* em um único conjunto de dados e a concatenação das colunas de conteúdo de interesse, o que facilita a análise subsequente. Já o módulo de extração permitiu identificar padrões e elementos relevantes nos dados coletados.

Ambos os módulos foram desenvolvidos em *Python*, uma linguagem de programação muito usada em análise de dados. Para identificar padrões nos dados, foram utilizadas expressões regulares adaptadas para cada tipo de IoC procurado. A seguir está a expressão regular utilizada para buscar IoCs do tipo e-mail:

```
(r"[a-zA-Z0-9.]+@[a-zA-Z0-9]+.[a-zA-Z]+(.[a-zA-Z]+)*")
```

Conforme mencionado na Seção 1, uma parte dos IoCs foi extraída com o auxílio do *ioc-finder*, versão 7.2.4, uma ferramenta de código aberto desenvolvida por Forrest Hightower [Hightower 2017] e disponível no *GitHub https://github.com/fhightower/ioc-finder*. A integração dessa ferramenta no projeto permitiu ampliar a busca e extração de tipos de indicadores relevantes, otimizando a análise de potenciais ameaças. Vale ressaltar que, neste trabalho, o foco está na extração de IoCs do tipo atômico.

A Tabela 1 mostra os tipos de IoCs que foram buscados em cada *post*, bem como a ferramenta usada na busca. O sistema criou uma coluna para cada tipo de IoC definido na Tabela 1, com o objetivo de registrar sua presença ou ausência em cada *post*. Adicionalmente, uma outra coluna denominada *IOC* foi criada para indicar se pelo menos um IoC foi encontrado no *post*. Inicialmente, todos os valores dessa coluna foram definidos como *NÃO*.

Tabela 1. Tipos de IoCs procurados e a ferramenta de extração utilizada

Tipo de IoC	**Ferramenta de Busca**
URL	Própria
E-mail	Própria
Domínio	Própria
Hash | MD5, SHA1, SHA256, SHA512 e SSDEEP	IoC-Finder
IPv4	Própria
IPv6	IoC-Finder
ASN	IoC-Finder
CVE	Própria
MAC	IoC-Finder
Registry Key Path	IoC-Finder

Em seguida, o sistema percorreu cada *post* e para aqueles que continham pelo menos um IoC, a coluna correspondente foi marcada com o valor *1*, enquanto a coluna *IOC* foi atualizada para *SIM*. Essa marcação tem como finalidade criar uma base de dados rotulada, permitindo a identificação de quais tipos de IoCs estão presentes em cada *post*. Essa base de dados será utilizada em análises posteriores e poderá ser compartilhada com outros pesquisadores mediante solicitações.

A Figura 2 mostra a marcação em dois *posts*. No *post* de ID 828, foi encontrado pelo menos um IoC do tipo *IP* e pelo menos um do tipo *URL*, logo, as colunas correspondentes foram marcadas com o valor *1*. Consequentemente, a coluna *IOC* foi atualizada para *SIM*. No *post* de ID 829, não foram encontrados IoCs, e portanto nenhuma coluna foi marcada. A coluna *IOC* permaneceu como *NÃO*. Todos os IoCs encontrados foram extraídos e salvos em arquivos de texto, sendo um arquivo para cada tipo de IoC.

ID	category	title	content	answers	tags	created_at	IOC	IP	URL	EML	HSH	CVE	DOM	ASN	IP6	MAC	RKP
828	Knowledge and info	IP DESTE SITE!!!	eu tentei pegar o ip deste site https://www.[redacted]com	[{'user': {'title': 'Patrimô	['ajuda', 'ip', 'hackings',	2020-08-27	SIM	1	1								
829	Other	quem é s t a c k z?	eu vi q é um youtuber ai sla mas pq quando falam aqui geralmente falam mal de	[{'user': {'title': None,	['stackz', 'respostas-ocultas',	2020-08-09	NÃO										

Figura 2. Marcações feitas para indicar a presença/ausência e o tipo de IoC encontrado nos *posts*

4.3. Etapa III - Análise de IoCs

Na terceira etapa, realizou-se uma análise quantitativa e empírica dos IoCs extraídos, com o objetivo de identificar informações relevantes em *posts* da *Dark Web* que possam auxiliar a comunidade de segurança da informação.

Durante o estudo, diversas informações relevantes foram extraídas, e as seguintes métricas foram apuradas:

1. Quantidade de *posts* nos quais foi encontrado pelo menos um tipo de IoC;
2. Quantidade de *posts* nos quais foi encontrado mais de um tipo de IoC;
3. Número de *posts* nos quais cada tipo de IoC foi encontrado;
4. Quantidade total de cada tipo de IoC extraído;
5. Percentual de IPs, URLs e domínios maliciosos obtidos por meio da *API VirusTotal*;
6. Análise quantitativa dos endereços de e-mail encontrados;
7. Incidência de IoCs por categoria dos *posts*;
8. Relação entre a ocorrência de IoC e a quantidade de interações nos *posts*.

5. Resultados

Nesta seção, apresentam-se os resultados da extração e análise dos IoCs. A base de dados analisada contém 26.994 *posts* extraídos de dois fóruns da *Dark Web*: o *Hidden Answers* e o *Deep Answer*, conforme já mencionado na Subseção 4.1

A Tabela 2 mostra a quantidade de *posts* coletados, o período de coleta e o idioma das mensagens dos dois fóruns que compõem a base de dados. Os períodos de coleta não foram uniformes devido aos períodos de inatividade nos fóruns. Os resultados serão apresentados de acordo com as questões de pesquisa apresentadas da Seção 1, sendo: Incidência de IoCs nos *posts* dos fóruns analisados (Subseção 5.1), Tipos de IoCs mais Frequentes (Subseção 5.2) e Fator que influencia a incidência de IoCs nos *posts* dos fóruns analisados (Subseção 5.3).

Tabela 2. Detalhes da base de dados analisada

Fórum	**Período de Coleta**	***Posts***	**Idioma**
Hidden Answers	Entre 26/11/2016 e 12/04/2021	19.654	Português do Brasil
Hidden Answers	Entre 31/07/2021 e 15/07/2022	6.682	Português do Brasil
Hidden Answers	Entre 29/01/2022 e 09/09/2022	312	Inglês
Deep Answers	Entre 24/08/2021 e 14/09/2022	242	Português do Brasil
Deep Answers	Entre 24/08/2021 e 06/09/2022	51	Inglês
Deep Answers	Entre 14/02/2022 e 19/09/2022	53	Espanhol
	Total de *posts*:	**26.994**	

5.1. Incidência de IoCs nos *posts* dos fóruns analisados

A primeira questão de pesquisa diz respeito à incidência de IoCs em fóruns da *Dark Web*. Dos 26.994 *posts* presentes na base de dados, em 7.083 foi encontrado pelo menos um tipo de IoC, o que representa um pouco mais de 26%. Esses resultados respondem à primeira questão de pesquisa, fornecendo informações sobre a presença de IoCs em fóruns da *Dark Web*.

A Tabela 3 oferece informações mais detalhadas sobre a quantidade de *posts* em que foram identificados IoCs. Um total de 7.083 *posts* apresentaram IoCs, sendo que em 6.645 deles foi identificado apenas um tipo de IoC. Em 421 *posts*, foram encontrados dois tipos de IoCs, enquanto em 16 *posts* foram identificados três tipos. Chama atenção o fato de que em apenas 1 *post* foram encontrados cinco tipos diferentes de IoCs: *IP, URL, E-mail, Domínio e ASN*.

Tabela 3. Quantidade de *posts* em que foram encontrados IoCs

Quantidade de Posts	**Tipos de IoC Encontrados**
6.645	1
421	2
16	3
1	5
Posts com algum tipo de IoC: 7.083 = (26,24%)	
Posts com mais de um tipo de IoC: 438 = (1,62%)	

5.2. Tipos de IoCs mais Frequentes

A segunda questão de pesquisa busca identificar os tipos mais frequentes de IoCs encontrados nos *posts*. Dentre os IoCs identificados, a expressiva maioria correspondeu a *URL*, seguida por *E-mail* e *Domínio*. Por outro lado, *CVE* e *Registry Key Path* tiveram menor incidência. Essa distribuição dos tipos de IoCs é destacada na Tabela 4.

Todas as URLs, endereços IPv4 e domínios extraídos foram verificados utilizando a *API VírusTotal* – uma plataforma online que, dentre outras funções, permite a verificação de alguns tipos de IoCs em busca de *malwares* e outras ameaças de segurança cibernética. Os resultados dessas verificações estão apresentados na Tabela 5, na qual as URLs apresentaram um percentual malicioso de 10,38%, enquanto os domínios e os endereços IPv4 apresentaram 11,90% e 18,64% respectivamente. É importante destacar que o percentual de URLs consideradas maliciosas neste estudo foi semelhante ao percentual observado por [Niakanlahiji et al. 2019] em uma análise preliminar de URLs

Tabela 4. Distribuição dos tipos de IoCs encontrados e extraídos

Tipo de IoC		Quantidade Extraída		Encontrado em
URL		9.795		6.267 *posts*
E-mail		1.177		774 *posts*
Domínio		332		292 *posts*
Hash	MD5	84	185	160 *posts*
	SHA1	87		
	SHA256	7		
	SHA512	3		
	SSDEEP	4		
IPv4		59		30 *posts*
ASN		8		5 *posts*
IPv6		8		4 *posts*
CVE		3		3 *posts*
MAC		6		3 *posts*
Registry Key Path		3		2 *posts*

extraídas do *Twitter*, na qual também foi identificado um índice de cerca de 10% de URLs maliciosas.

Tabela 5. Resultado da verificação de IoCs no *Virus Total*

IoC	Verificados	Ativos	Maliciosos	% Malicioso
URL	9.795	3.746	389	10,38%
Domínio	332	311	37	11,90%
IPv4	59	59	11	18,64%

Vale ressaltar que os endereços de *hash* também foram verificados na *API Virus-Total*, porém não foi identificado qualquer conteúdo malicioso. Além disso, foi realizada uma consulta às chamadas *Rainbow Tables*, que são tabelas que armazenam uma extensa lista de senhas juntamente com os seus respectivos valores de *hashes*, gerados por meio de um algoritmo específico; entretanto, nenhum resultado relevante foi encontrado. Também foi realizada uma análise quantitativa dos endereços de e-mail, devido ao fato de serem um dos IoCs mais frequentes. O objetivo era determinar quais tipos de e-mails foram encontrados. Vale ressaltar que, após uma análise minuciosa, alguns endereços foram descartados por não corresponderem a endereços de e-mail, apesar de possuírem um formato semelhante. Os resultados mostraram que a grande maioria dos provedores de e-mail encontrados durante a análise são focados em segurança e anonimato dos usuários, conforme é mostrado na Tabela 6.

5.3. Fator que influencia a incidência de IoCs nos *posts* dos fóruns analisados

Para responder à terceira questão de pesquisa, que busca saber se existe algum fator que influencia a incidência de IoCs nos *posts*, foram realizadas duas análises: a primeira relacionada à categoria dos *posts* e a segunda ao número de interações recebidas por cada *post*. Nesse contexto, as interações representam o total de respostas e comentários obtidos por cada mensagem inicial.

Na análise por categoria, as dezenas de categorias existentes foram agrupadas em apenas duas: *Computação* e *Outras*. Nessa análise, todos os *posts* que pertenciam à alguma categoria relacionada à computação foram agrupados nessa categoria. Já os *posts*

Tabela 6. Análise quantitativa de endereços de e-mail

Quantidade	Percentual	Tipo
247	34,84%	Provedor de e-mail de código aberto que se diz seguro (criptografia de ponta a ponta)
154	21,72%	Provedor de e-mails descartáveis
103	14,53%	Comercial
103	14,53%	Serviço de e-mail da rede *TOR*
58	8,18%	Diversos
32	4,51%	Provedor de e-mail anônimo da *Darknet*
5	0,71%	Privado
4	0,56%	Permite registro e uso na rede *TOR* e outros serviços de privacidade
3	0,42%	Gerencia e-mails da *Surface* e da *Dark Web*
709	100,00%	

cujas categorias não possuíam nenhuma relação com computação foram agrupados na categoria *Outras*. Esse agrupamento busca facilitar a análise e a identificação de categorias que possam demandar mais ou menos atenção em análises futuras. Em seguida, foi apurada a incidência de IoCs em relação as duas novas categorias.

Os resultados mostraram que a incidência de IoCs em *posts* da categoria *Computação* é quase duas vezes maior do que a outras categorias. Vale ressaltar que embora a incidência de IoCs em outras categorias seja muito menor, ainda assim ela é significativa. A Tabela 7, mostra o resultado dessa análise.

Tabela 7. Análise da incidência de IoCs em relação às categorias *Computação* e *Outras*

Categoria Computação 9.561 *Posts* (35,42%)	
Incidência de IoC	
Posts	**Tipos de IoC Encontrados**
3.339	1
221	2
7	3
1	5
Posts com algum tipo de IoC 3.568 = (37,32%)	
Posts com mais de um tipo de IoC 229 = (2,4%)	

Outras Categorias 17.433 *Posts* (64,58%)	
Incidência de IoC	
Posts	**Tipos de IoC Encontrados**
3.306	1
200	2
9	3
Posts com algum tipo de IoC 3.515 = (20,16%)	
Posts com mais de um tipo de IoC 209 = (1,2%)	

Já na análise por interações, verificou-se o número máximo e mínimo de interações em cada *post*, bem como a média e o desvio padrão em relação aos *posts* que possuem IoC e aos que não possuem. O objetivo dessa análise foi verificar se existe alguma relação entre o número de interações e a presença de IoC nos *posts*. O racional por trás dessa análise é verificar se *posts* com algum IoC e, potencialmente maliciosos, possuem algum grau maior de interação do que outros tipos de *posts*.

Os resultados revelaram que uma maior quantidade de interações não implica necessariamente na presença de IoCs. A Tabela 8 apresenta o resultado dessa análise, mostrando que a média e o desvio padrão das interações nos *posts* sem IoC foram ligeiramente

maiores. Após a aplicação do teste estatístico *ANOVA* (Tabela 9) em ambas as amostras, seguido por uma análise *Post-Hoc* (Tabela 10), foi constatada uma diferença estatisticamente significativa entre as médias dos dois grupos. O teste estatístico *ANOVA* revelou um valor de *p-valor* inferior a 0,05, o que indica uma diferença significativa e, consequentemente, rejeita-se a hipótese nula, confirmando essa diferença na análise *Post-Hoc*.

Tabela 8. Análise da quantidade de interações nos *posts* com e sem IoC

Posts	Média	Desvio Padrão	Máximo	Mínimo
SIM (tem IoC)	6,52	5,10	49	0
NÃO (não tem IoC)	7,08	5,29	51	0

Tabela 9. Resultado do teste estatístico ANOVA em relação às interações nos *posts* com e sem IoC

Variável	N. de Observações	R^2	R^2 Ajustado	F-Estatístico	P-Valor
Interações	26.994	0,002	0,002	59,72	1,13e-14

Tabela 10. Resultado da análise *Post-Hoc* em relação às interações nos *posts* com e sem IoC

Diferença Média	P-Ajustado	Valor Mínimo	Valor Máximo	Rejeitar
-0,56	0,0	-0,702	-0,418	Sim

Os histogramas e *boxplots* nas Figuras 3 e 4, respectivamente, auxiliam na visualização dos resultados obtidos nos testes aplicados. Essas visualizações confirmam que a quantidade de interações nos *posts* que contêm IoCs não é superior, como possivelmente imaginado, em comparação com aqueles que não possuem. Portanto, dentre os fatores avaliados, constatou-se que apenas a categoria exerce influência na incidência de IoCs nos *posts* dos fóruns analisados.

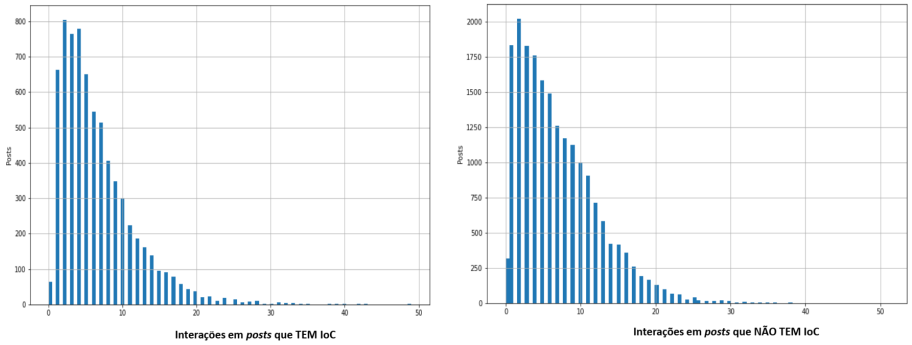

Figura 3. Histograma das interações nos *posts* com e sem IoC

6. Conclusão

Este artigo teve como foco principal a extração e análise de IoCs em fóruns da *Dark Web*, com o objetivo de verificar a incidência de IoCs nessa fonte de dados, os tipos de IoC mais frequentes e se existe algum fator que influencia a incidência de IoCs nos *posts* desses fóruns. A base de dados contou com 26.994 *posts* coletados de dois fóruns públicos de boa movimentação na *Dark Web*.

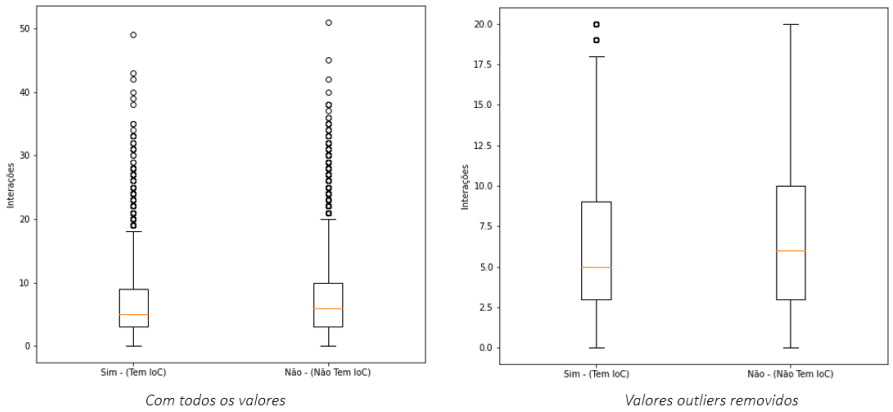

Figura 4. Boxplot das interações nos *posts* com e sem IoC

Com relação a primeira questão de pesquisa, que trata da incidência de IoCs nos *posts*, os resultados mostraram que em mais de 26% dos *posts* foram encontrado pelo menos um tipo de IoC. Já em relação a segunda questão de pesquisa, dos tipos de IoCs mais frequentes, URL representa uma grande maioria, seguida por e-mail e domínio, respectivamente. Uma verificação utilizando a API do *VirusTotal*, constatou como maliciosos: 10,38% das URLs, 11,90% dos domínios e 18,64% dos IPv4. Em relação a terceira questão de pesquisa, do fator que influência a incidência de IoCs nos *posts*, uma análise feita por categoria, onde os *posts* foram agrupados em duas categorias: *Computação* e *Outras*, revelou que a incidência de *IoCs* em *posts* cujas categorias estão relacionadas à computação é quase duas vezes maior do que aqueles que não são. No entanto, embora a incidência de IoCs em outras categorias não relacionadas à computação seja menor, essas categorias não devem ser descartadas, pois o número de IoCs encontrados nelas é significativo. Em relação ao número de interações que os *posts* recebem ficou constatado que um número maior de interações não significa necessariamente uma maior incidência de IoC. Portanto, conclui-se que a *Dark Web* pode ser uma boa fonte de dados para aquisição de informações de inteligência de segurança da informação contra as ameaças e incidentes de segurança.

Como trabalho futuro, pretende-se aplicar algoritmos de aprendizado de máquina supervisionado na base de dados que já se encontra pré-rotulada, assim como em outras bases de diferentes fontes, a fim de criar modelos de detecção de *posts* maliciosos. Um outro ponto que será explorado é a presença de IoCs em *posts* maliciosos, ou seja, de que forma os IoCs impactam na identificação de tais *posts*.

Referências

Akhgar, B., Gercke, M., Vrochidis, S., and Gibson, H. (2021). *Dark Web Investigation*. Springer.

Al-Ramahi, M., Alsmadi, I., and Davenport, J. (2020). Exploring hackers assets: topics of interest as indicators of compromise. In *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, pages 1–4.

Asiri, M., Saxena, N., Gjomemo, R., and Burnap, P. (2023). Understanding indicators of compromise against cyber-attacks in industrial control systems: a security perspective. *ACM transactions on cyber-physical systems*.

Basheer, R. and Alkhatib, B. (2021). Threats from the dark: a review over dark web investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications*, 2021:1–21.

Bradbury, D. (2014). Unveiling the dark web. *Network security*, 2014(4):14–17.

Brooks, C. (2021). Alarming cybersecurity stats: What you need to know for 2021. `https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=6ae7f87158d3`. Accessed: 2022-1-20.

Caballero, J., Gomez, G., Matic, S., Sánchez, G., Sebastián, S., and Villacañas, A. (2023). The rise of goodfatr: A novel accuracy comparison methodology for indicator extraction tools. *Future Generation Computer Systems*, 144:74–89.

Cubrilovic, N. (2018). Rockyou hack: From bad to worse. dec. 2009. *URl: http://techcrunch. com/2009/12/14/rockyou-hack-securitymyspace-facebook-passwords*.

Dong, F., Yuan, S., Ou, H., and Liu, L. (2018). New cyber threat discovery from darknet marketplaces. In *2018 IEEE Conference on Big Data and Analytics (ICBDA)*, pages 62–67. IEEE.

Hightower, F. (2017). Observable finder, 2017. *URL https://github.com/fhightower/ioc-finder*.

Jo, H., Lee, Y., and Shin, S. (2022). Vulcan: Automatic extraction and analysis of cyber threat intelligence from unstructured text. *Computers & Security*, 120:102763.

Niakanlahiji, A., Safarnejad, L., Harper, R., and Chu, B.-T. (2019). Iocminer: Automatic extraction of indicators of compromise from twitter. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 4747–4754. IEEE.

Olhar Digital (2021). ANPD abre investigação de vazamento de dados de quase todos os brasileiros. `https://olhardigital.com.br/2021/02/04/noticias/anpd-abre-investigacao-de-vazamento-de-dados-de-quase-todos-os-brasileiros/`. Accessed: 2022-1-20.

Saleem, J., Islam, R., and Kabir, M. A. (2022). The anonymity of the dark web: A survey. *IEEE Access*, 10:33628–33660.

Sapienza, A., Bessi, A., Damodaran, S., Shakarian, P., Lerman, K., and Ferrara, E. (2017). Early warnings of cyber threats in online discussions. In *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, pages 667–674. IEEE.

Sarkar, S., Almukaynizi, M., Shakarian, J., and Shakarian, P. (2019). Predicting enterprise cyber incidents using social network analysis on dark web hacker forums. *The Cyber Defense Review*, pages 87–102.

Zhang, P., Ya, J., Liu, T., Li, Q., Shi, J., and Gu, Z. (2019). imcircle: Automatic mining of indicators of compromise from the web. In *2019 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6. IEEE.