CRIMES CIBERNÉTICOS: UM PANORAMA GERAL SOBRE AS PRINCIPAIS AMEAÇAS

MARCELO SILVEIRA[1]
CLAYTON EDUARDO DOS SANTOS[2]

RESUMO

Os avanços tecnológicos de nossa época têm beneficiado a sociedade de diversas maneiras, especialmente no que tange ao uso da Internet, que tornou a comunicação entre os indivíduos mais dinâmica, eficiente e prática. Tais benefícios podem ser observados por exemplo, no crescente uso das plataformas de e-commerce, redes sociais, educação à distância, Internet das Coisas, dentre outros recursos disponibilizados na grande rede mundial de computadores.
Da mesma forma que a sociedade se beneficia destes avanços, a criminalidade igualmente se aproveita das novas tecnologias para também inovar a forma com que violam os direitos dos cidadãos. O presente trabalho tem como objetivo exibir um panorama geral sobre as principais ameaças enfrentadas pelas organizações públicas e privadas.

Palavras-chave: crimes cibernéticos, segurança cibernética, sistemas de detecção de intrusão.

[1] Especialização em Gestão Estratégica da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Estado de São Paulo – Câmpus de Bragança Paulista – IFSP. Curso de Pós-Graduação Lato Sensu (IFSP). E-mail:marcelo.silveira.br@gmail.com
[2] Professor Doutor, Instituto Federal de Educação, Ciência e Tecnologia do Estado de São Paulo – Câmpus de Bragança Paulista – IFSP. Curso de Pós-Graduação Lato Sensu (IFSP), e-mail: claytones@ifsp.edu.br.

CYBERCRIMES: A MAIN THREATS' GENERAL OVERVIEW

ABSTRACT

The technological advances of our days have benefited society in many ways, especially regarding the use of the Internet, which has made communication between individuals more dynamic, efficient and practical. Such benefits can be observed, for example, in the growing use of e-commerce platforms, social networks, distance education, Internet of Things, among other resources available on the great world wide web.

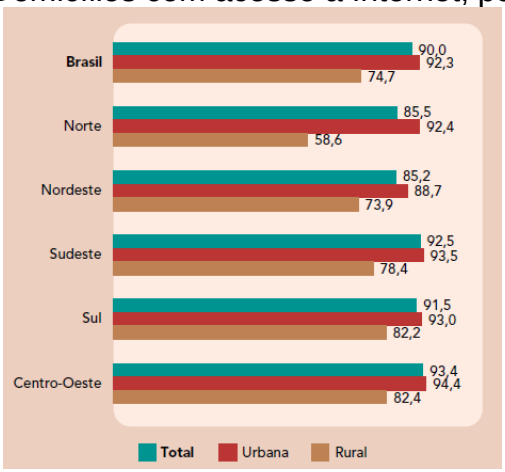
In the same way that society benefits from these advances, criminals also take advantage of new technologies to also innovate the way they violate citizens' rights. This work aims to provide with a general overview of the main threats faced by public and private organizations.

Keywords: *cybercrime, cybersecurity, intrusion detection systems.*

1. INTRODUÇÃO

Dados do IBGE demonstram que o acesso à Internet é uma realidade na vida da maioria dos brasileiros, conforme pode se constatar na Figura 1. Dos 72,9 milhões de domicílios estudados pela instituição em 2021 no Brasil, 90% utilizavam a Internet (IBGE, 2022). Milhões de pessoas utilizam-se dessas tecnologias para as mais diversas finalidades: enviar mensagens, conversar por chamadas de voz, assistir a vídeos, filmes e séries, enviar e receber e-mails (IBGE, 2022).

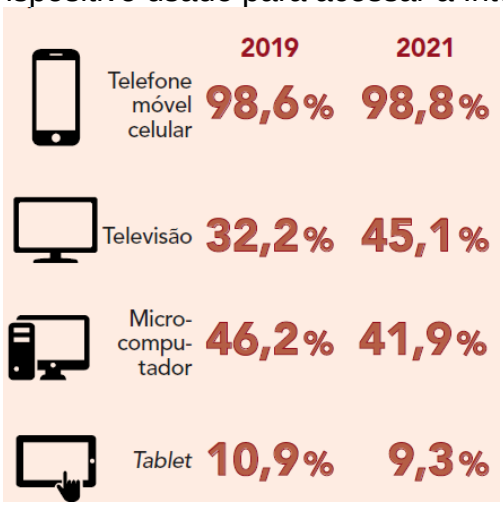
Figura 1 - Domicílios com acesso à Internet, por situação (%)



Fonte: (IBGE, 2022)

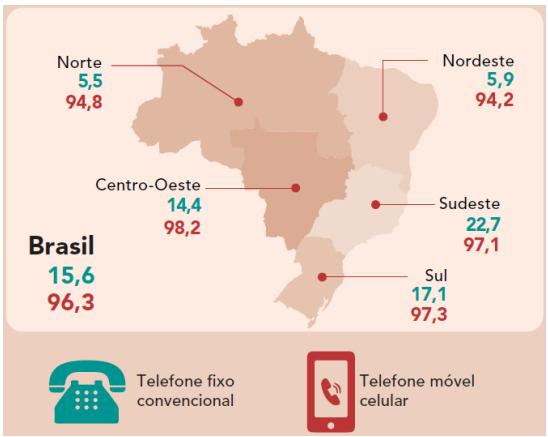
Um dos instrumentos essenciais para esta inclusão digital é popularização do uso dos dispositivos móveis, especialmente pelo seu custo bem inferior, se comparado a computadores, aparelhos televisores e *tablets*. As Figuras 2 e 3 demonstram bem este cenário.

Figura 2 - Dispositivo usado para acessar a Internet



Fonte: (IBGE, 2022)

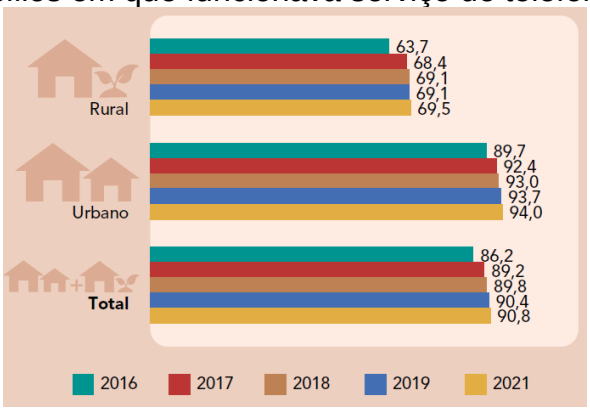
Figura 3 - Domicílios com telefone fixo convencional e com telefone móvel celular



Fonte: (IBGE, 2022)

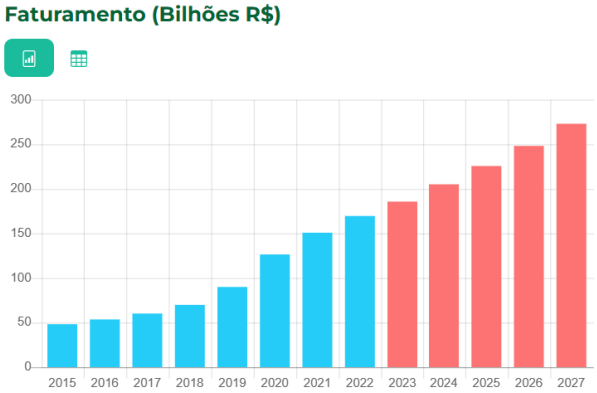
Embora grande parte da população tenha acesso à Internet e a telefones celulares móveis, pode ser verificado na Figura 4 que ainda existem muitas oportunidades de expansão dos serviços de banda larga móvel, especialmente nas áreas urbanas.

Figura 4 - Domicílios em que funcionava serviço de telefonia móvel celular



Fonte: (IBGE, 2022)

Figura 5 - Faturamento e Projeções para Ecommerce



Fonte: ASSOCIAÇÃO BRASILEIRA DE COMÉRCIO ELETRÔNICO (2023)

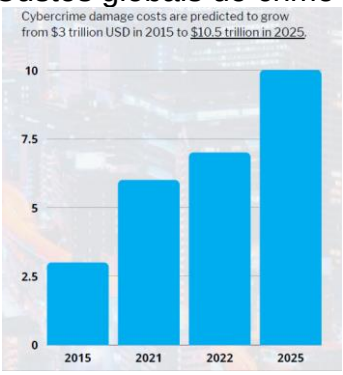
As empresas também se beneficiaram desta evolução da inclusão digital da população brasileira, pois necessitam expor sua marca ou oferecer seus serviços através da Internet, com o risco de não sobreviver à concorrência se não o fizerem. Muitos têm sido beneficiados com esse avanço tecnológico, especialmente aqueles que aderiram ao comércio eletrônico, pois em 2022, as vendas pela *Internet* no Brasil atingiram o valor de R$ 169,59 bilhões (ASSOCIAÇÃO BRASILEIRA DE COMÉRCIO ELETRÔNICO, 2023).

As projeções de faturamento das vendas pela Internet seguem a mesma tendência que o número de usuários, conforme demonstra o **Erro! Fonte de referência não encontrada.**, que mostra o faturamento do *e-commerce* brasileiro de

2015 a 2022, bem como as projeções para os próximos 6 anos, demonstrando que as perspectivas são animadoras para o setor de comércio eletrônico.

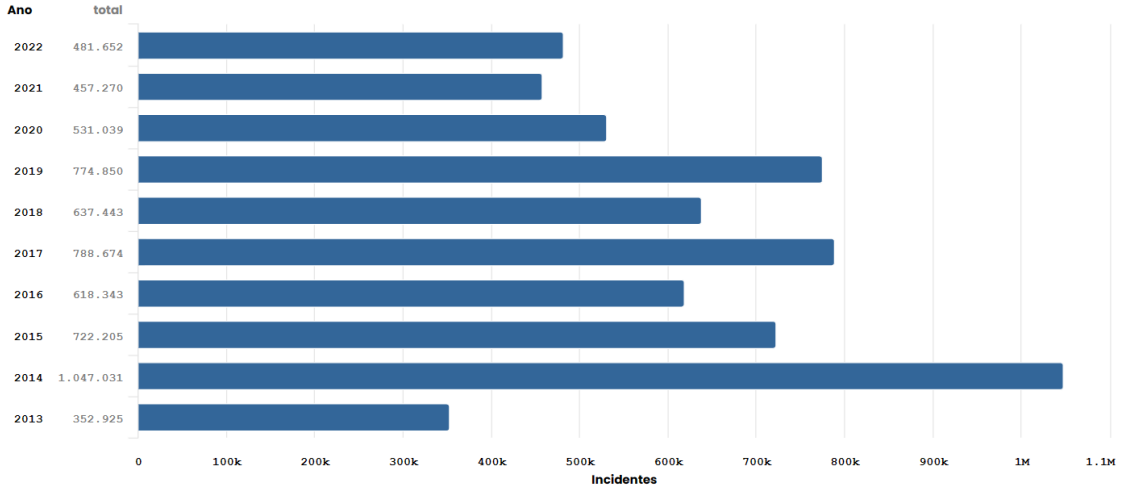
Embora a consolidação da *Internet* como ferramenta de comércio traga faturamento e lucro para muitas empresas e benefícios e facilidades para seus usuários, não são poucos os que são prejudicados por esses avanços tecnológicos, pois criminosos se aproveitam de suas habilidades com a tecnologia para cometerem terrorismo e guerra cibernéticos, *cyber-espionagem*, pornografia infantil, *cyber-bullying, phishing* (AL-KHATER, AL-MAADEED, *et al.*, 2020) etc., objetivando denegrirem a imagem, furtarem recursos, distorcerem e danificarem informações, impossibilitarem prestações de serviços eletrônicos, dentre outras atividades ilícitas. As projeções de prejuízos decorrentes dos crimes cibernéticos globais em 2021 somam 6 trilhões de dólares (JAVED, AHMED, *et al.*, 2022) e sua projeção no mundo inteiro para os próximos anos pode ser exemplificada pela Figura 6. A Figura 7 mostra os incidentes reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil de 2013 a 2022.

Figura 6 - Custos globais do crime cibernético



Fonte: (MORGAN, 2022)

Figura 7 - Notificações de incidentes recebidos pelo CERT.br de 2013 a 2022

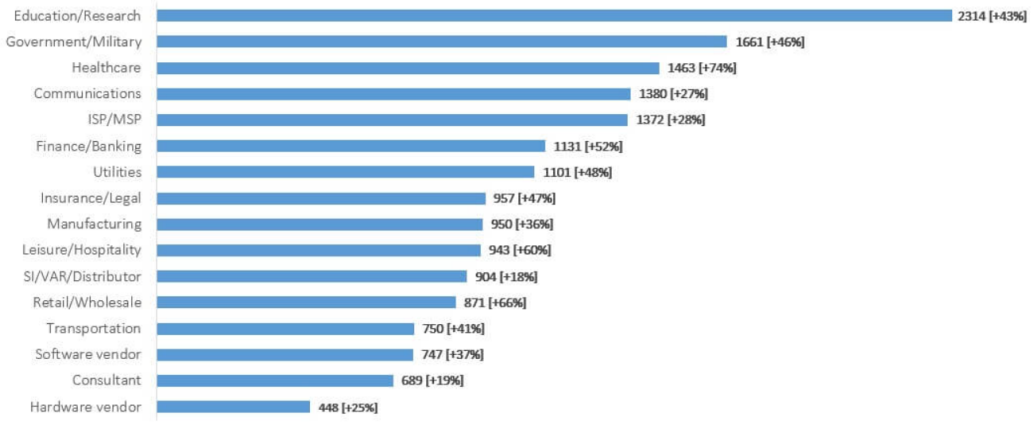


Fonte: (CENTRO DE ESTUDOS, 2023)

Conforme os crimes cibernéticos evoluem em natureza e complexidade e os prejuízos aumentam, a necessidade por ferramentas, algoritmos e soluções forenses para detectar e deter estes indivíduos cresce dia a dia. Como uma resposta a esta necessidade, governos e entidades privadas estão encarando este problema de uma forma mais séria e estão investindo na busca do desenvolvimento e aplicação de leis e padrões, com vistas a enfrentar essas ameaças e proteger os cidadãos e as entidades privadas e públicas para que possam usufruir dos benefícios que essas inovações propiciam (JAVED, AHMED, *et al.*, 2022).

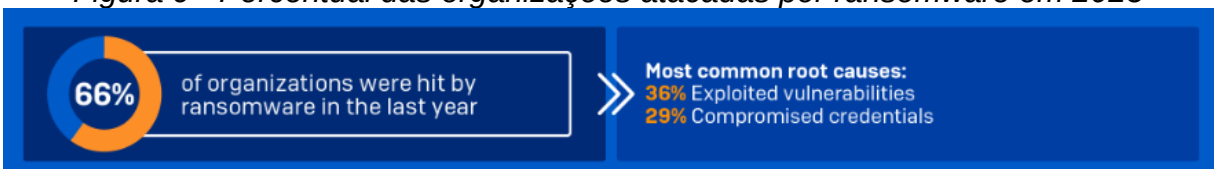
A Figura 8 mostra que o setor de educação e pesquisa foi o que mais sofreu ataques globalmente em 2022, seguido pelos setores governamentais/militares e hospitalares. Segundo Patel (2023), 94% das organizações relataram algum ataque sofrido em 2022. A Figura 9 mostra que o *ransomware* foi o ataque mais relatado por elas, globalmente, em 2023, enquanto a Figura 10 exibe o restante dos tipos de ataques sofridos, em valores percentuais. A Microsoft reconhece que 50% dos seus esforços para recuperação de ataques cibernéticos são relacionados a ataques de *ransomware* (MICROSOFT, 2022).

Figura 8 - Média semanal de ataques relatados em 2022 por Setor, em comparação a 2021 [%]



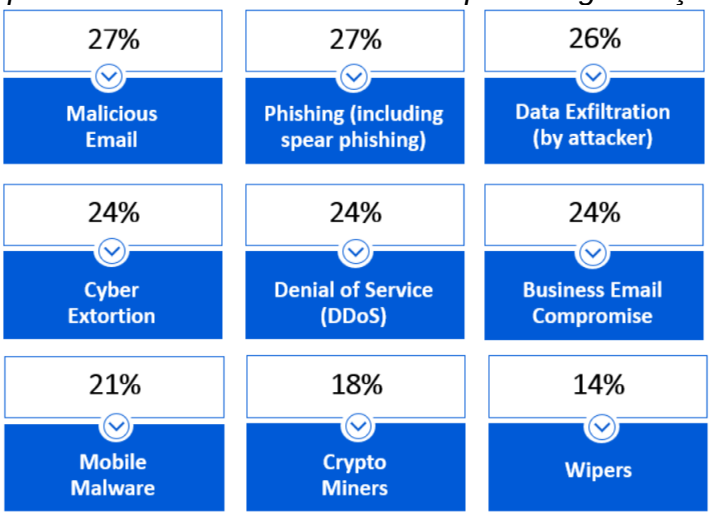
Fonte*:* (TEAM, 2023)

Figura 9 - Percentual das organizações atacadas por ransomware em 2023



Fonte*:* (SOPHOS, 2023)

Figura 10 - Ataques não-ransomware relatados pelas organizações em %

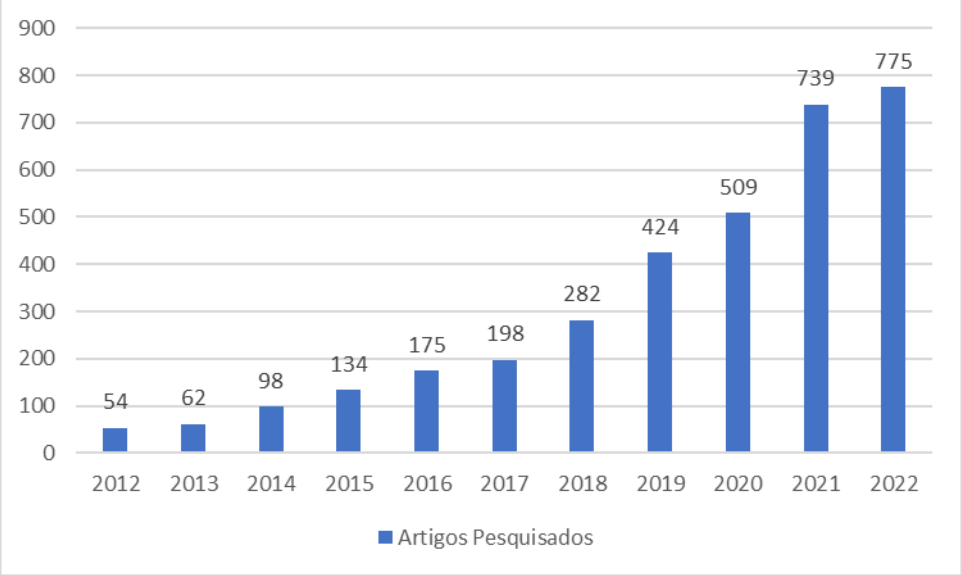


Fonte*:* (PATEL, 2023)

Dada a relevância deste tema, pode-se constatar na Figura 11 que pela evolução do número de artigos escritos sobre este assunto há uma tendência de as

tecnologias evoluírem e as ameaças aumentarem, e assim segurança cibernética e crimes cibernéticos serão cada vez mais estudados no meio acadêmico.

Figura 11 - Artigos sobre crimes cibernéticos



Fonte: Autoria própria

O objetivo deste trabalho é listar os tipos de ataques mais usados em nossos dias baseado na bibliografia estudada, oferecendo assim um panorama geral sobre as principais ameaças cibernéticas enfrentadas em nossos dias.

2. METODOLOGIA APLICADA

Este trabalho é uma pesquisa de abordagem qualitativa, de natureza aplicada e objetivo exploratório. Tem natureza aplicada pois aborda um problema relevante, que são os crimes cibernéticos. Este tipo de prática criminosa tem trazido prejuízos à sociedade, independentemente do nível das pessoas afetadas, haja visto as projeções das perdas estimadas mencionadas na introdução.

Esta pesquisa também tem um objetivo exploratório, pois busca explorar as maneiras com que os crimes cibernéticos são cometidos. Adota ainda o procedimento de pesquisa bibliográfica de artigos de revistas e periódicos científicos, na busca de informações sobre o tema, conforme explicado a seguir:

Foram definidas as Palavras-Chave a serem usadas nas pesquisas;

- *Cybercrime, cybersecurity, crimes cibernéticos*

Escolheu-se um período de abrangência para este estudo

- *2012 a 2023*

Determinou-se, igualmente, o Tipo de Publicação

- *Journals ou Magazines;*

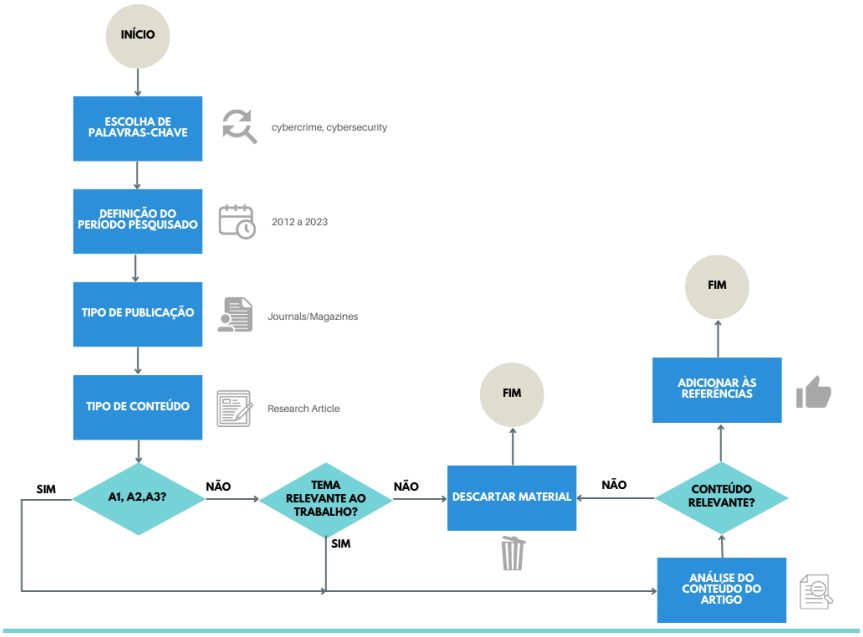
Em algumas Bases, como a ACM, houve a escolha do Tipo de Conteúdo

a. *Research Article*

Por fim, selecionaram-se revistas e periódicos com classificações A1, A2, A3. Obs.: Artigos que não se encontravam nesta classificação, mas continham material relevante para a discussão foram utilizados, como exceção.

A lista e análise foram então adicionados às referências bibliográfica. Todo o processo é ilustrado na Figura 12.

Figura 12 - Fluxo do processo de aquisição de Bibliografia



Fonte: Autoria própria.

3. TIPOS DE CRIMES CIBERNÉTICOS

Antes de mais nada é muito importante definir o que é o crime cibernético, que pode ser definido como:

> o mau uso de dados, computadores, sistemas de informação e do espaço cibernético (redes, Internet etc.) para lucro pessoal, financeiro ou psicológico. (ARIEF e BIN ADZMI, 2015).

A justiça brasileira já reconhece em sua legislação alguns tipos de crimes cibernéticos:

> 1. pornografia infantil por meio de sistema de informática (art. 241-B do Estatuto da Criança e do Adolescente – ECA), 2. corrupção de menores em salas de bate-papo da Internet (art. 244-B, § 1º, do ECA), 3. violação de direitos de autor de programa de computador (art. 12 da Lei Federal n. 9.609/98), 4. inserção de dados falsos em sistema de informações (art. 313-A do Código Penal), 5. crimes contra equipamentos de voto (art. 72 da Lei Federal n. 9.504/97), 6. invasão de dispositivo informático (art. 154-A do Código Penal), 7. interrupção ou perturbação do serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 266 do Código Penal – nova redação) (BECHARA e FLORES, 2020), 8. interceptar comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei (art. 10 da Lei 9.296/96), 9. modificação ou alteração não autorizada de sistema de informações (art. 313-B do Código Penal) (DE LIMA FILHO, 2021).

AL-KHATER et al. (2020) classificam os crimes cibernéticos em 9 categorias: 1. terrorismo cibernético, que é relacionado à violência contra pessoas e suas posses; 2. guerra cibernética, quando os criminosos causam problemas políticos entre países; 3. espionagem cibernética, que é o roubo de informações sensíveis de uma empresa para o benefício de seus concorrentes; 4. pornografia infantil, que se refere a imagens, vídeos e áudios contendo crianças em situação de nudez, ou roupas e posições que tenham cunho sexual; 5. *bullying* cibernético, que envolve qualquer atividade que cause humilhação, assédio moral, manipulação psicológica e até atividades danosas como roubo de cartão de crédito, de identidade, perseguição; 6. *phishing*, onde os criminosos normalmente enviam e-mails falsos com o objetivo de manipular suas vítimas a lhes entregarem dados sensíveis; 7. Ataques de injeção de *SQL*, quando o ataque causa danos aos bancos de dados através de códigos *SQL*, podendo inclusive roubar informações sensíveis e 8. ataques futurísticos, que se referem a ataques a tecnologias recentes, como *Wi-Fi*, dispositivos médicos, robôs, drones, carros autônomos etc.

4. FASES DE UM ATAQUE

Um ataque cibernético pode ser desdobrado em 7 fases:

Na fase de reconhecimento os criminosos coletam informações sobre vulnerabilidades desconhecidas pelos seus alvos para mais tarde definirem a estratégia de ataque a ser utilizada. Em seguida, na fase de armamento, de posse das vulnerabilidades identificadas, eles desenvolvem as ferramentas que serão utilizadas para acessar remotamente a máquina da vítima (*worm*, vírus etc.). Durante a fase de entrega, a ferramenta é transmitida aos sistemas a serem violados e logo depois eles assumem o controle sobre suas vítimas e passam a explorar seus dados (Explorar, Controlar). Assim, os criminosos estão prontos para executarem seus códigos para furtarem e destruírem os dados delas (Executar, Manter) (TIDJON, FRAPPIER e MAMMAR, 2019).

Figura 13 - As 7 fases de um ataque cibernético

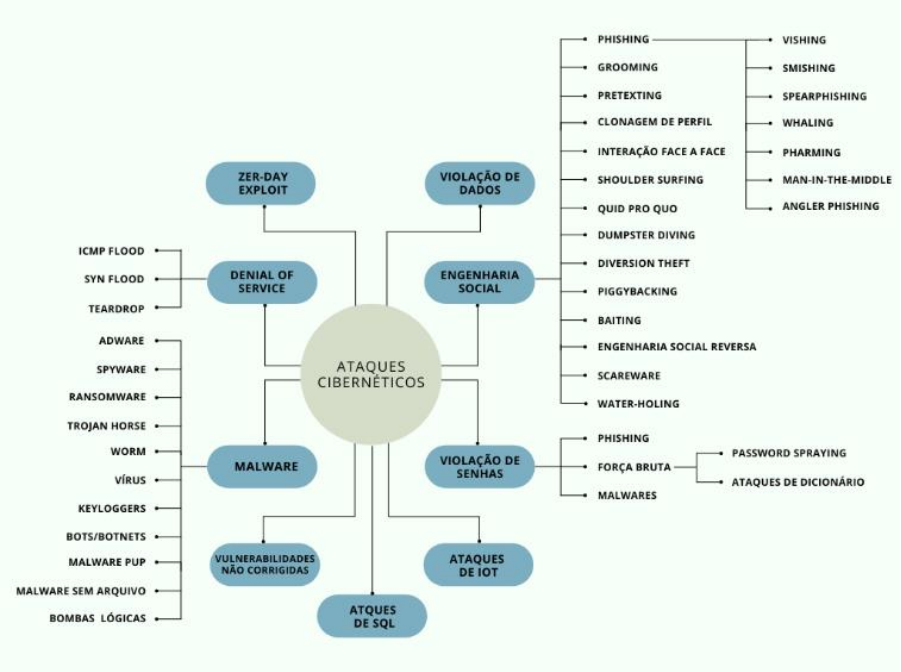
Fonte: Autoria própria.

5. TIPOS DE ATAQUE

Para se impedir ou minimizar os prejuízos decorrentes dos crimes cibernéticos, as autoridades e empresas se esforçam por identificar como os criminosos realizam

seus atos. Este trabalho de identificação é prejudicado pelo volume de inovações tecnológicas postas em funcionamento e escala, pois elas permitem novas oportunidades de desenvolvimento de técnicas que visam prejudicar os usuários finais. Com base na literatura pesquisada, pode-se identificar os seguintes tipos de ataques cibernéticos:

Figura 14 - Tipos de Ataques Cibernéticos



Fonte: Autoria própria

5.1. DoS/DDoS – *Denial of Service/Distributed Denial of Service* – Este tipo de ataque visa indisponibilizar o acesso a recursos através de um número muito grande de requisições de acesso ao servidor (AL-KHATER, AL-MAADEED, *et al.*, 2020). O DoS é o segundo maior tipo de ataque relatado no CERT.br (2023) e a Figura 15 mostra a evolução do mesmo de 2016 a julho/2023. Os ataques desta natureza podem ser feitos através dos seguintes métodos:

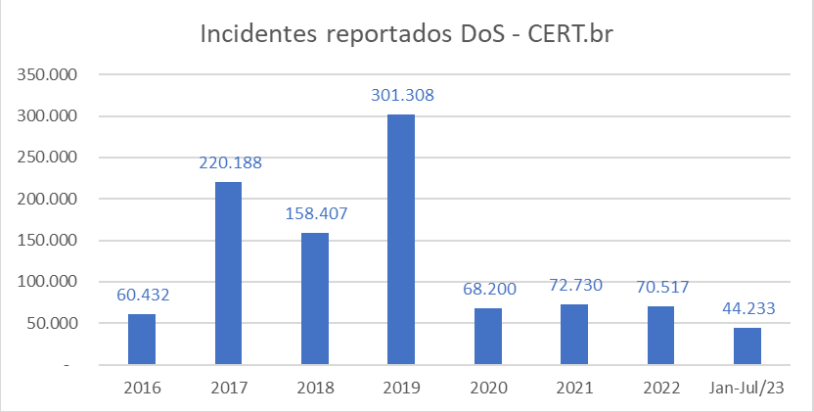
5.1.1. Ataque de inundação ICMP ou ataque *Smurf* – Os atacantes sobrecarregam o servidor com muitas mensagens ICMP (diagnóstico e

erros de rede), para que este processe todas até que entre em colapso (AL-KHATER, AL-MAADEED, *et al.*, 2020).

5.1.2. Ataque de inundação *SYN* – Os criminosos enviam um alto volume de mensagens (*SYN*) de solicitação de conexão inicial com o objetivo de paralisar o servidor (CLOUDFLARE, 2023).

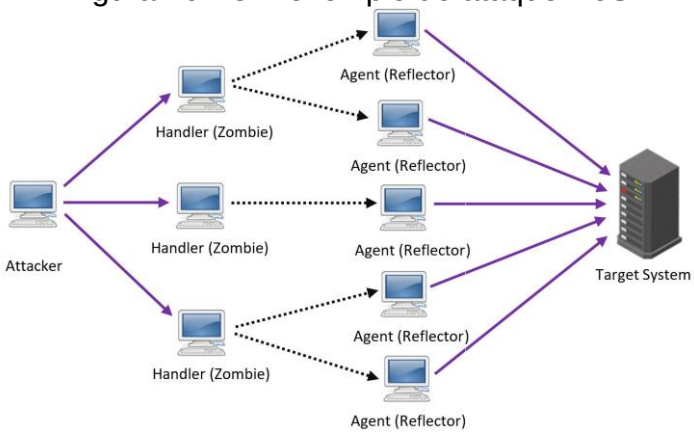
5.1.3. Ataque *TEARDROP* – Os servidores são paralisados através de *packets* enviados de forma desorganizada ou sobreposta que os forçam a consumir seus recursos na tentativa de montá-los (AL-KHATER, AL-MAADEED, *et al.*, 2020).

Figura 15 - Incidentes de DoS reportados ao CERT.br



Fonte dos dados: (CENTRO DE ESTUDOS, 2023)

Figura 16 - Um exemplo de ataque DoS



Fonte: (AL-KHATER, AL-MAADEED, et al.*, 2020)*

5.2. Engenharia Social (SYAFITRI, SHUKUR, *et al.*, 2022)

A engenharia social manipula suas vítimas para adquirir informações sensíveis ou dinheiro. Esta técnica é utilizada também como porta de entrada para a utilização de outras técnicas, como o *malware*. O desafio neste tipo de ataque consiste na prevenção, porque não basta apenas aplicar ferramentas de *hardware e software*, pois o ataque é realizado sobre os indivíduos que operam os recursos de *hardware e software*. A lista abaixo descreve os tipos de ataque mais usados em engenharia social:

5.2.1. *Phishing* – São mensagens maliciosas que iludem suas vítimas, que consistem em instruções ou sugestões enviadas para manipulá-las. Elas normalmente tomam a forma de mensagens de *e-mail* e *sites* fraudulentos. O *Phishing* pode assumir as seguintes formas:

Vishing – Nessa forma de *phishing* ligações telefônicas são usadas para se obter as informações desejadas, sem que as vítimas percebam;

Smishing – Esta técnica utiliza-se de mensagens SMS enviadas para telefones de conhecimento público ou números aleatórios;

Spearphishing – É o uso de mensagens de e-mail cujos alvos são pessoas ou grupos específicos e possuem um conteúdo de interesse para os indivíduos visados.

Whaling – Semelhante ao *spearphishing*, sendo que os alvos são indivíduos em funções de liderança e alto escalão dentro das organizações;

Pharming – Os criminosos desviam o tráfego da Internet para sites falsificados para conseguirem aplicar seus golpes;

Man-in-the-middle – O atacante se coloca entre a vítima e o emissor legítimo de uma mensagem real. Ele, então, intercepta a mensagem e a modifica, infectando-a com um *Trojan Horse*.

Angler phishing – O indivíduo clona perfis de atendimento ao cliente das redes sociais de empresas. Ele procura clientes destas empresas que

manifestaram algum tipo de insatisfação nas redes sociais e, passando-se pela empresa, fingem atender a esta insatisfação e furtam informações e/ou dinheiro.

5.2.2. *Grooming* –

> É uma técnica recente de Engenharia Social onde os criminosos utilizam-se de técnicas de psicologia e de tecnologia de informação para obter informações pertinentes à pedofilia, especialmente entre adolescentes. Na maioria das vezes estas conversas podem acontecer em redes sociais, mas podem também se utilizar de *e-mail*, SMS, ligação telefônica e/ou outros meios de comunicação (SYAFITRI, SHUKUR, *et al.*, 2022).

5.2.3. *Pretexting* ou Pretexto – Os interesses e atividades das vítimas são estudados e pesquisados pelos atacantes em sites, redes sociais etc. De posse dessas informações, eles as abordam com um assunto de interesse comum (emprego, prêmios, oferta de ajuda etc.) com o objetivo de manipulá-las e obterem informações sigilosas e/ou dinheiro.

5.2.4. Clonagem de perfil – Esta técnica de Engenharia Social utiliza informações públicas para fingir ser uma pessoa de destaque através da clonagem de seu perfil, com o objetivo de abordar seguidores e obter deles dados sensíveis e dinheiro.

5.2.5. Interação face a face – As vítimas, aqui, são abordadas pessoalmente no ‘mundo real’ em conversas em que os indivíduos exploram suas vulnerabilidades para tomarem vantagem e obterem informações importantes.

5.2.6. *Shoulder surfing* – Esta técnica não necessita de habilidades especiais, pois explora a alienação das vítimas com as redondezas. Basicamente o indivíduo mal-intencionado procura olhar sobre os ombros delas (como o nome sugere) e visualizar informações que possam possibilitar alguma vantagem.

5.2.7. Ataques *Quid Pro Quo* – De alguma forma o *hacker* envolve sua vítima de forma que ela lhe peça um favor para resolver um problema que não consegue. Ele então se oferece para solucionar a questão, desde que ela ser comprometa a entregar-lhe algumas informações, dinheiro ou algo que interesse ao *hacker*.

5.2.8. *Dumpster diving* (mergulho no lixo) – A negligência humana em destruir documentos e informações não mais utilizáveis, físicos ou não, possibilita que os criminosos vasculhem lixeiras físicas ou digitais e encontrem dados sensíveis.

5.2.9. *Diversion theft* (roubo por desvio) – Os criminosos roubam as informações de envio de produtos, através de *phishing* e outras técnicas, desviam a entrega deles para novos endereços e entregam produtos falsos para as vítimas. Nos novos endereços eles recebem os produtos desviados.

5.2.10. *Piggybacking* – É a exploração dos acessos de funcionários/administradores para conseguir violar e roubar os recursos e informações sensíveis da empresa.

5.2.11. *Baiting* – Este método tira vantagem da curiosidade das pessoas. Os *hackers* se utilizam de mídias digitais em *pen drives* e/ou cartões de memória contaminados por *malware* ou *trojans*. Utilizam-se também de textos muito atrativos que atraem o tráfego de cliques para os links contaminados.

5.2.12. Engenharia Social Reversa – Aqui os *hackers* sabotam, avisam e corrigem: eles criam problemas nos dispositivos usados pelas vítimas, que procuram ajuda; logo eles avisam da existência do problema e oferecem suporte. A vítima, então, aceita esta ajuda e concede acesso ao criminoso, que rouba os dados ou instala aplicativos que contaminarão toda a rede para coletar tudo o que lhe for interessante.

5.2.13. *Scareware* ou Janelas *Pop-Up* – os atacantes instalam *scripts* de janelas *pop-up* que aparecem repentinamente ou quando um usuário executa alguma ação. Estas mensagens possuem cores chamativas e sons assustadores, confundindo o usuário para que ele clique em *links* que instalam vírus em seus computadores e permitem que seus dados sejam roubados.

5.2.14. *Water-Holing* (bebedouro) – Funciona de forma semelhante aos caçadores que espreitam suas presas em fontes de água ou poços. Da mesma forma os criminosos infectam *sites* com alto índice de tráfego e simplesmente aguardam que usuários desavisados acessem o mesmo e executem os códigos para que eles iniciem suas tentativas de acesso.

5.3. Ataques de *Malware*

> Os *malwares* são ataques de *software* contra aplicativos e *softwares*, fazendo-os funcionarem de forma diferente da esperada, causando prejuízos (FALOWO, POPOOLA, *et al.*, 2022).

A lista a seguir exibe os tipos mais comuns de *malware* (KASPERSKY, 2023):

5.3.1. *Adware* – Os *adwares* surgem muitas vezes na forma de janelas de *pop-up* que exibem publicidade indesejada e muitas vezes maliciosa, redirecionando para sites de publicidade e capturando os dados do usuário;

5.3.2. *Spyware* – Tipo de *malware* que fica oculto no dispositivo, roubando informações sensíveis. Ele pode se espalhar automaticamente, explorando vulnerabilidades de segurança ou disfarçado em *softwares* legítimos;

5.3.3. *Ransomware* – *Software* malicioso que bloqueia o acesso do usuário ao seu sistema ou nega acesso aos seus dados até que um resgate seja pago;

5.3.4. *Trojan Horse* (Cavalo de Tróia) – Apresentado disfarçado de *software* legítimo, uma vez instalado concede acesso aos *hackers*, que por sua vez

acessam e roubam os dados de suas vítimas. Eles não se espalham automaticamente, pois precisam de um hospedeiro para poderem funcionar;

5.3.5. *Worms* – É um programa independente que explora vulnerabilidades e se replica para outros dispositivos sem a necessidade de intervenção do usuário. É um dos tipos mais comuns de *malware* e é utilizado normalmente para danificar sistemas, executar *ransomwares*, roubar informações e outras violações;

5.3.6. Vírus – É um código inserido em um *software* legítimo. Quando este é instalado ou executado, o vírus é ativado e passa a acessar e roubar dados, lançar ataques DDoS ou até mesmo *Ransomwares*. Eles necessitam que o *software* hospedeiro seja executado para realizarem suas atividades;

5.3.7. *Keyloggers* – São aplicativos que monitoram as atividades das pessoas que acessam o sistema. Podem ser benéficos, no caso de pais que desejam monitorar as atividades de seus filhos pequenos na Internet, mas podem ser usados de forma criminosa, roubando senhas, dados bancários e informações sigilosas de suas vítimas;

5.3.8. *Bots e Botnets* – O dispositivo que foi vítima de um ataque de *malware* e que está sob o controle do invasor é chamado de *bot*. Ele pode também ser usado para contaminar e controlar outros dispositivos, criando uma rede de *bots* ou *botnet*, para a aplicação de ataques DDoS, *Spam*, *Phishing* e propagação de *malwares*.

5.3.9. *Malware PUP* – Sigla para o Inglês *Potentially Undesired Program,* são *malwares* normalmente instalados na forma de barras de pesquisa, publicidade, barras de ferramentas e *pop-ups* que não têm nenhuma relação com o aplicativo que se desejava baixar. Surgem na forma de ‘*combos’* em *sites* de *download* de aplicativos.

5.3.10. *Malwares* sem arquivos – Infecta os dispositivos através de programas legítimos, mas não deixa rastros, pois não precisa ser instalado diretamente na máquina. Ele atua diretamente na memória RAM e não toca nos discos rígidos, sendo, portanto, muito difícil de ser detectado pelos sistemas de detecção de intrusão (IDS). É uma modalidade cujo uso tem crescido nos últimos dias, por causa dessa característica.

5.3.11. Bombas Lógicas – São *malwares* que são acionados de acordo com condições lógicas predeterminadas. Estes programas causam danos aos discos rígidos, dados de aplicativos ou outros problemas;

5.4. Violação de dados

> É a exposição intencional ou inadvertida de informações confidenciais e/ou privativas que podem levar a graves prejuízos financeiros e danos à reputação das organizações atingidas tanto a médio como longo prazo (FALOWO, POPOOLA, *et al.*, 2022).

5.5. Ataques de violação de senha (SECURITY BOULEVARD, 2022)

São tentativas de conseguir acesso não autorizado a sistemas e dispositivos por meio de violação e/ou descoberta de senhas e códigos de acesso. Estas tentativas podem usar as seguintes técnicas:

5.5.1. *Phishing* – a maioria das técnicas descritas anteriormente;

5.5.2. Ataques de Força Bruta – Ataques que visam roubar as senhas utilizando a técnica de tentativa e erro que podem ser:

Password Spraying – Os criminosos utilizam um grande número de senhas comumente usadas pelas pessoas em uma grande quantidade de contas. As tentativas são feitas em lote, para diminuir o risco de serem rastreados;

Ataques de Dicionário – Palavras comuns e frases de dicionário são colocadas numa lista e usadas para violar as senhas.

5.5.3. *Malwares* como os *Keyloggers*;

5.6. *Zero-Day Exploit* (Ataques de Dia-Zero) (KASPERSKY, 2023)

São ataques realizados em vulnerabilidades que ainda não foram descobertas pelos usuários e/ou pelos fornecedores dos sistemas de detecção de invasões, ou vulnerabilidades que acabaram de ser descobertas.

5.7. Exploração de vulnerabilidades não corrigidas (FALOWO, POPOOLA, *et al.*, 2022)

Neste ataque as vulnerabilidades são conhecidas pelos fornecedores e organizações, mas por restrições de orçamento, priorização e outros motivos, as empresas executam as correções nos itens mais prioritários enquanto os outros aguardam na fila. Estas vulnerabilidades são então descobertas e exploradas pelos hackers.

5.8. Ataques de *IoT* (FALOWO, POPOOLA, *et al.*, 2022)

A Internet das Coisas possibilitou uma conectividade sem precedentes entre dispositivos e a Internet. Devido a esta variedade de dispositivos, localidades, protocolos e plataformas, torna-se desafiador impedir que os criminosos obtenham sucesso em suas tentativas de invasão, pois o universo de possibilidades é imenso.

5.9. Ataques de *SQL Injection* (AL-KHATER, AL-MAADEED, *et al.*, 2020)

Nesta modalidade a base de dados é comprometida através de códigos *SQL* maliciosos que são inseridos nos campos de formulários, possibilitando a invasão, roubo e destruição do banco de dados.

Um outro aspecto importante a ser observado, especialmente considerando o grande número de aparelhos celulares em uso no Brasil, são as vulnerabilidades decorrentes da obsolescência destes dispositivos. O governo brasileiro revelou que só em 2020 foram registrados mais de 234 milhões de acessos móveis (GOV.BR,

2022). Um estudo realizado pela fundação Getúlio Vargas revelou que existiam 249 milhões de *smartphones* em uso no Brasil em 2022 (VARGAS, 2023). Entretanto, a agência Brasil relatou que são somente 152 milhões de pessoas com acesso à Internet (LEÓN, 2021). Esta discrepância pode indicar que muitos destes celulares podem ter sido passados de pais para filhos e, por conta do tempo de uso já podem ter se tornado obsoletos. O problema principal da obsolescência é que celulares com versões desatualizadas do Android tornam-se muito mais vulneráveis a ataques que os aparelhos mais novos, que recebem de forma recorrente e sistemática atualizações de segurança, em vista às novas técnicas de ataque desenvolvidas pelos criminosos (NOGUEIRA, 2020). Este fato, por si só, deve ser considerado como uma grande vulnerabilidade que também precisa ser levada em conta pelas autoridades e entidades que trabalham para coibir os crimes cibernéticos.

6. CONCLUSÕES

Diante do grande avanço tecnológico dos últimos dez anos percebemos que a sociedade passou a desfrutar de uma qualidade de vida nunca antes vista. Comunicações, transações e notícias em tempo real e escala global não são mais uma inovação, já fazem parte do cotidiano de qualquer cidadão médio.

É também assustadora a velocidade com que os crimes cibernéticos evoluem, em número de eventos, escala de magnitude de danos e inovações tecnológicas aplicadas a seus atos. A comunidade científica não tem poupado esforços para se manter atualizada frente às ameaças que evoluem dia a dia e as tecnologias baseadas em Inteligência Artificial combinadas com outras tecnologias parecem ser um novo conjunto de ferramentas a ser utilizado nos próximos anos.

Para próximos trabalhos, há uma lacuna a ser preenchida no tocante aos métodos e ferramentas usados na Perícia Forense Computacional, que usa de forma posterior muitas ferramentas de detecção de intrusões e que também imprime grandes esforços para detectar, denunciar e punir os criminosos cibernéticos. Outro ponto a ser estudado em trabalhos futuros são os métodos de processamento de eventos de *streaming*, que também são alvos constantes de ataques e que merecem atenção especial.

REFERÊNCIAS

AL-KHATER, W. A. et al. Comprehensive Review of Cybercrime Detection Techniques. **IEEE Access**, v. 8, p. 137293-137311, 2020. ISSN ISSN: 2169-3536.

ARIEF, B.; BIN ADZMI, M. A. Understanding Cybercrime from Its Stakeholders' Perspectives: Part 2–Defenders and Victims. **IEEE Security & Privacy**, v. 13, p. 84-88, March 2015. ISSN ISSN: 1558-4046.

ASSOCIAÇÃO BRASILEIRA DE COMÉRCIO ELETRÔNICO, A. Previsão de vendas no e-Commerce para os Próximos 5 anos. **ABCOMM FOREKAST**, 2023. Disponivel em: <https://dados.abcomm.org/previsao-de-vendas-online>.

BECHARA, F. R.; FLORES, D. M. CRIMES CIBERNÉTICOS: QUAL É O LUGAR DO CRIME PARA FINS DE APLICAÇÃO DA PENA E DETERMINAÇÃO DA COMPETÊNCIA JURISDICIONAL? **Revista Direito Mackenzie**, v. 13, 2020. ISSN ISSN: 2317-2622.

CENTRO DE ESTUDOS, R. E. T. D. I. D. S. N. B. Incidentes Notificados ao CERT.br, 2023. Disponivel em: <https://stats.cert.br/incidentes/>.
CLOUDFLARE. Ataque de inundação SYN, 2023. Disponivel em: <https://www.cloudflare.com/pt-br/learning/ddos/syn-flood-ddos-attack/>.

DE LIMA FILHO, P. R. A. O DIREITO PENAL NA QUARTA REVOLUÇÃO INDUSTRIAL: A expansão razoável frente aos crimes cibernéticos. **Delictae (Online)**, v. 6, 2021. ISSN ISSN: 2526-5180.

FALOWO, O. I. et al. Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. **IEEE Access**, v. 10, p. 134038-134051, 2022. ISSN ISSN: 2169-3536.

GOV.BR. Anatel divulga relatório da telefonia móvel relativo a 2020. **Notícias**, 2022. Disponivel em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-divulga-relatorio-da-telefonia-movel-relativo-a-2020>.

IBGE. IBGE PAÍSES - BRASIL. **IBGE PAÍSES**, 2022. Disponivel em: <https://paises.ibge.gov.br/#/dados/brasil>.

JAVED, A. R. et al. A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. **IEEE Access**, v. 10, p. 11065-11089, 2022. ISSN ISSN: 2169-3536.

KASPERSKY, A. O. L. Centro de Recursos, 2023. Disponivel em: <https://www.kaspersky.com.br/resource-center/threats/types-of-malware; https://www.kaspersky.com.br/resource-center/definitions/zero-day-exploit>.

LEÓN, L. P. Brasil tem 152 milhões de pessoas com acesso à internet. **Agência Brasil**, 2021. Disponivel em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-08/brasil-tem-152-milhoes-de-pessoas-com-acesso-internet>.

MICROSOFT. Microsoft Digital Defense Report 2022, 2022. Disponivel em: <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022>.

MORGAN, S. BOARDROOM CYBERSECURITY 2022 REPORT. **Cybersecurity Ventures**, 2022. Disponivel em: <https://cybersecurityventures.com/cybercrime-magazine-archives/#home/?view_1_search=statistics&view_1_page=1>.

NOGUEIRA, L. Celulares com Android ultrapassado podem representar riscos; entenda. **Olhar Digital**, 2020. Disponivel em: <https://olhardigital.com.br/2020/05/12/seguranca/celulares-com-android-ultrapassado-podem-representar-riscos-entenda/>.

PATEL, R. Defensores x Adversários: a corrida de cibersegurança em duas velocidades em 2023. **Products & Services**, 2023. Disponivel em: <https://news.sophos.com/pt-br/2023/04/04/defensores-x-adversarios-a-corrida-de-ciberseguranca-em-duas-velocidades-em-2023/>.

SECURITY BOULEVARD, E. What is a Password Attack in Cyber Security?, 2022. Disponivel em: <https://securityboulevard.com/2022/05/what-is-a-password-attack-in-cyber-security/>.

SOPHOS. The State of Ransomware 2023. **State of Ransomware**, 2023. Disponivel em: <https://assets.sophos.com/X24WTUEQ/at/h48bjq7fqnqp3n5thwxtg4q/sophos-the-state-ransomware-2023-infographic-1200-1200px_2x.png>.

SYAFITRI, W. et al. Social Engineering Attacks Prevention: A Systematic Literature Review. **IEEE Access**, v. 10, p. 39325-39343, 2022. ISSN ISSN: 2169-3536.

TEAM, C. P. R. Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. **Security**, 2023. Disponivel em: <https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/>.

TIDJON, L. N.; FRAPPIER, M.; MAMMAR, A. Intrusion Detection Systems: A Cross-Domain Overview. **IEEE Communications Surveys & Tutorials**, v. 21, p. 3639-3681, 2019. ISSN ISSN: 1553-877X.

VARGAS, F. G. Uso de TI no Brasil: País tem mais de dois dispositivos digitais por habitante, revela pesquisa, 2023. Disponivel em: <https://portal.fgv.br/noticias/uso-ti-brasil-pais-tem-mais-dois-dispositivos-digitais-habitante-revela-pesquisa>.