DO VÍRUS À DEFESA

Um Olhar Crítico sobre a Segurança Cibernética na Era da Informação

Iraê César Brandão

2025

http://doi.org/10.29327/7566630

doi 10.29327/7566630

Do Vírus à Defesa: Um Olhar Crítico sobre a Segurança Cibernética na Era da Informação

From Virus to Defense: *A Critical Look at Cybersecurity in the Information Age*

Iraê César Brandão[1]

[1]iraecbrandao@gmail.com.br

https://orcid.org/0000-0002-2079-0615

Abstract: *This essay takes an introductory look at computer viruses, covering their definition, the ways in which they spread, the most common types and their impact on digital environments. Based on a theoretical and exploratory review, it discusses signs of infection, dissemination, protection, and practices such as ethical hacking. The methodology was based on a bibliographical survey and qualitative analysis of secondary sources, with a focus on accessibility to readers with diverse levels of familiarity. The study also highlights the importance of digital education in prevention. One limitation is the lack of empirical data and technical depth. Even so, it contributes by broadening the critical view of digital security and encouraging conscious practices. It concludes that strengthening information security requires technical solutions as well as educational actions and effective public policies.*

Keywords: *Computer viruses, Malware, Cyber security, Digital infection, Antivirus.*

Resumo: Este ensaio analisa, de forma introdutória, os vírus de computador, abordando definição, formas de propagação, tipos mais comuns e impactos em ambientes digitais. A partir de revisão teórica e exploratória, se discutem sinais de infecção, disseminação, proteção e práticas como *ethical hacking*. A metodologia se baseou em levantamento bibliográfico e análise qualitativa de fontes secundárias, com foco na acessibilidade a leitores com diferentes níveis de familiaridade. O estudo também destaca a importância da educação digital na prevenção. Como limitação, se aponta a ausência de dados empíricos e aprofundamento técnico. Ainda assim, contribui ao ampliar o olhar crítico sobre a segurança digital e fomentar práticas conscientes. Se Conclui que fortalecer a segurança da informação exige tanto soluções técnicas quanto ações educativas e políticas públicas eficazes.

Palavras-chave: Vírus de computador, *Malwar*e, Segurança cibernética, Infecção digital, Antivírus.

---

[1] Graduado em Gestão de TI pela UNICSUL; MBA Executivo em Segurança Cibernética pela FI; MBA Executivo em Gestão Estratégia de *Marketing*, Planejamento e Inteligência Competitiva pela FI; Especialista em: Linguagens e suas Tecnologias e o Mundo do Trabalho pela UFPI; Matemática e suas Tecnologias pela UFPI; Uso Educacional da Internet pela UFLA; Docência do Ensino Superior e Neuropsicologia pela Faculeste; Docência em Administração pela Faculeste; Docência para Educação Profissional e Tecnológica pela Faculeste; Empresário no ramo de Tecnologia e Segurança da Informação (2001-2025); Professor na rede Estadual de Ensino disciplina Tecnologia da Informação em Curso Técnico.

1. Introdução

A segurança digital é uma preocupação central na era da informação, especialmente devido aos vírus de computador, que são elementos maliciosos capazes de comprometer o desempenho e a integridade dos sistemas. Este artigo propõe uma análise introdutória sobre o que são os vírus, como se manifestam, seus diferentes tipos, modos de infecção e estratégias de prevenção.

Com o aumento da conectividade global e da dependência de sistemas digitais, cresce a necessidade de entender os mecanismos que colocam em risco a segurança cibernética. Compreender o funcionamento dos vírus e como se propagam é relevante para promover ambientes digitais mais seguros e resilientes.

Diante do cenário de ameaças digitais crescentes, é essencial compreender as definições, comportamentos, formas de contágio e impactos dos vírus de computador na integridade de sistemas e dados. Este ensaio visa oferecer uma visão acessível sobre os vírus, bem como elementos complementares à segurança digital, abordando suas formas de disseminação, principais tipos, métodos de prevenção, além de aspectos como a classificação de hackers e estratégias de engenharia social utilizadas para facilitar infecções.

Nesse cenário, duas questões orientam este estudo: O que caracteriza um vírus de computador e de que forma ele compromete sistemas e informações? E quais são os principais tipos de vírus e as estratégias mais eficazes para sua prevenção e combate? A partir dessas indagações, se pretende não apenas identificar os riscos técnicos, mas também refletir sobre a importância da educação digital na formação de usuários mais críticos, conscientes e preparados para enfrentar os desafios da era da informação.

Durante a realização deste ensaio, algumas limitações foram identificadas e impactaram diretamente a profundidade da análise proposta. Em primeiro lugar, por se tratar de uma abordagem introdutória e de caráter teórico, não houve a utilização de dados empíricos ou estatísticos atualizados, tampouco a inclusão de estudos de caso que pudessem ilustrar, de forma prática, a ocorrência de infecções por vírus de computador em diferentes cenários.

Outrossim, a opção por tornar o conteúdo acessível a leitores em processo de alfabetização digital levou à adoção de uma abordagem mais generalista, o que implicou na limitação do uso de terminologias técnicas e na exclusão de análises mais específicas, como aquelas relacionadas à engenharia reversa, criptografia ou ao comportamento de *malwares*[2] em ambientes corporativos. Ao se somar a isso a rapidez com que a tecnologia evolui, o que faz com que determinadas informações se tornem rapidamente obsoletas diante das constantes transformações nas estratégias de ataque e nas formas de atuação dos vírus digitais.

2. Estudos Relacionados

2.1. Definição e Funcionamento dos Vírus de Computador

Um vírus de computador é um programa malicioso e inteligente, desenvolvido com o propósito de se replicar automaticamente e se propagar entre arquivos e sistemas,

[2] *Malware* (abreviação de *software* malicioso) - é qualquer *software* projetado para prejudicar um computador ou rede, roubando informações, causando danos ou perturbando o funcionamento normal [Palatty 2025].

muitas vezes sem o conhecimento do usuário. Sua atuação pode comprometer seriamente o funcionamento dos dispositivos, causando perda de desempenho, vazamento de informações sensíveis ou até mesmo a destruição de dados relevantes. Esse tipo de *software* atua de maneira estratégica, operando na maioria das vezes por meio da inserção em *arquivos hospedeiros*[3] (*e.g.,* com extensões de arquivo como: *.exe*[4], *.com*[5], *.bat*[6]). O vírus é ativado quando o usuário executa o arquivo infectado, momento em que o código malicioso é carregado e começa a agir de forma autônoma, demonstrando características de um programa inteligente ao se adaptar a diferentes ambientes e mecanismos de segurança [Stallings 2017].

Os vírus de computador são programas maliciosos desenvolvidos para se infiltrar em sistemas, se replicar e causar danos ou roubo de informações. O termo *vírus* foi inspirado nos vírus biológicos, devido à sua capacidade de se multiplicar e infectar outros arquivos ou dispositivos. De acordo com publicação da *University of Houston-Downtown*, " [...] os vírus impactaram um número significativo de computadores nos últimos anos. Se Estima que existam mais de 10.000 vírus conhecidos no mundo, e a cada mês são descobertos mais de 200 novos tipos [...]" [UHD 2025a tradução nossa].

Esse crescimento constante demonstra como a ameaça digital está em evolução contínua, exigindo medidas rigorosas de prevenção e atualização constante dos sistemas de segurança. A luta contra os vírus e outros programas maliciosos é um desafio permanente na proteção de dados e na manutenção da integridade dos ambientes digitais.

2.2. Formas de Contágio

Inicialmente disseminados por disquetes, hoje os vírus são amplamente propagados pela internet, especialmente por anexos de *e-mail*, *downloads* suspeitos, dispositivos USB infectados e até por redes locais. A ativação exige, geralmente, a execução do código malicioso pelo usuário.

Em sua publicação sobre *Auditoria de Segurança*, Palatty (2025), em seu estudo embasado por pesquisas nas principais estatísticas sobre *malware*, chegou aos seguintes resultados de detecções:

> "[...] 560.000 novos *malwares* são detectados diariamente e existem atualmente mais de 1 bilhão de programas maliciosos. Só no primeiro semestre de 2022, ocorreram 236,7 milhões de ataques de *ransomware* em todo o mundo, com um custo médio de US$ 4,54 milhões por incidente [...] à medida que nos aproximamos de 2025, a ameaça de ataques de *malware* continua a pairar sobre organizações em todo o mundo, e especialistas preveem que a frequência desses ataques só aumentará nos próximos anos. É evidente que a segurança cibernética continua sendo uma preocupação crítica para empresas de todos os portes" [Palatty 2025 tradução nossa].

[3] Arquivos hospedeiros - para que um vírus possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado [Stallings 2017].

[4] Arquivo *.exe* - é o arquivo executável visto frequentemente em sistemas operacionais como o *Windows* [Stallings 2017].

[5] Arquivo *.com* - é um tipo de arquivo executável antigo, especialmente popular em sistemas operativos como MS-DOS e CP/M. Esses arquivos contêm instruções de máquina em formato binário e podem ser diretamente executados pelo sistema operativo [Stallings 2017].

[6] Arquivo *.bat* (também conhecido como arquivo *batch* ou script *BAT*) - é um arquivo de texto que o processador de linha de comando *cmd.exe*, do *Windows,* processa em lote. Com ele, o Prompt de Comando assume tanto o papel de interpretador quanto de ambiente de tempo de execução [Stallings 2017].

Outras formas de infecção de vírus é a utilização de emoções humanas para manipular vítimas, conforme o autor em Brandão (2025 p. 4), onde em seu estudo concluiu que: "[...] os *hackers* ou *crackers* usam emoções para manipular as vítimas e aumentar as chances de sucesso dos ataques de engenharia social [...]". Essa afirmação se baseia em seu estudo dos autores Daswani & Elbayadi (2021), Zetter, Wilson & Hadnagy (2014), Cole, Krutz & Conley (2005) e Mitnick & Simon (2002; 1963/2003), onde concluiu que:

> "[...] a engenharia social é uma técnica sofisticada e eficaz por explorar vulnerabilidades humanas, e não técnicas. Eles convergem ao afirmar que a psicologia humana é o elo mais frágil da segurança da informação - compreender sua manipulação é essencial tanto para proteger quanto para atacar" [Brandão 2025 p. 4].

Ibidem ainda afirma, conforme a análise feita dos autores estudados que:

> "[...] de forma unânime, as emoções como elementos centrais nos ataques de engenharia social. medo, urgência, culpa e curiosidade são apresentados como gatilhos emocionais explorados estrategicamente para burlar o senso crítico e a lógica das vítimas, facilitando o acesso não autorizado a dados e sistemas [...]" [Brandão 2025 p. 6].

2.3. Sinais de Infecção

Diversos indícios podem sinalizar a presença de um vírus [Fortinet 2022]:

- Desempenho lento do sistema;
- *Pop-ups*[7] indesejados;
- Fechamento automático de programas;
- Falhas de *login*[8] e desconexões;
- Falhas de inicialização ou desligamentos inesperados;
- Alterações na página inicial do navegador;
- Envio de *e-mails* não autorizados.

O autor deste ensaio, com vasta experiência em Tecnologia da Informação e Comunicação (TDICs), incluindo especialização em Segurança Cibernética e Gestão de Tecnologia da Informação, acumula mais de 25 anos de atividades profissionais dedicadas ao campo tecnológico. Com um histórico significativo em segurança da informação e eliminação de vírus em sistemas operacionais, o autor ressalta que os sinais de infecção, apesar de sua presença evidente em alguns casos, são frequentemente difíceis de detectar.

Muitos vírus são projetados para oferecer uma ilusão de conforto aos usuários de sistemas e *softwares*[9], tornando essencial uma proteção mais robusta dos equipamentos.

---

[7] *Pop-ups* (ou janelas de surgimento) - são janelas que aparecem de forma inesperada no seu navegador enquanto você navega na internet. Geralmente, são pequenas janelas que surgem no primeiro plano da tela, chamando a atenção do usuário [Stallings 2019; ANDERSON 2008].

[8] *Login* - se refere ao processo de autenticação de um usuário em um sistema ou aplicativo, geralmente utilizando um nome de usuário e senha. É o ato de fornecer credenciais para ter acesso a uma área restrita de um site, aplicativo ou sistema [Tanenbaum 2011; 2015].

[9] *Software* - em informática, se refere ao conjunto de instruções, dados e programas que fazem um computador funcionar, permitindo-lhe realizar tarefas específicas. É o oposto do *hardware*, que são os componentes físicos do computador. Em termos simples, o *software* é a parte *lógica* ou *intangível* do computador, enquanto o *hardware* é a parte física [Stallings 2019; Anderson 2008].

Isso pode ser alcançado através do uso de antivírus eficazes ou ferramentas tecnológicas especializadas, além da intervenção de profissionais com conhecimento adequado para garantir uma abordagem técnica e profissional na mitigação dessas ameaças (técnicas e estratégias utilizadas para minimizar os níveis de risco e reduzi-los a níveis toleráveis).

As observações do autor sobre a dificuldade de detecção de infecções por vírus e outras ameaças digitais encontram respaldo na literatura especializada. Bruce Schneier, uma das maiores autoridades internacionais em segurança da informação, argumenta que muitos sistemas operacionais e *softwares* transmitem aos usuários uma sensação falsa de segurança. Segundo ele, diversos *malwares* são projetados justamente para operar de forma discreta e imperceptível, criando uma *zona de conforto* enquanto exploram vulnerabilidades. Essa estratégia torna a detecção extremamente complexa para o usuário comum, exigindo ferramentas específicas e, muitas vezes, a intervenção de profissionais especializados [Schneier 2000].

De forma complementar, Mark Stamp enfatiza que a sofisticação dos códigos maliciosos atuais desafia tanto os sistemas automatizados quanto os usuários menos experientes. Em sua obra, o autor descreve como as técnicas de ofuscação e dissimulação tornam muitos vírus invisíveis aos antivírus tradicionais. Por isso, segundo o autor deste ensaio, é imprescindível que medidas de segurança cibernética sejam acompanhadas não apenas por soluções tecnológicas de proteção, mas também por conhecimento técnico qualificado. O profissional com know-how apropriado desempenha papel fundamental na análise e neutralização de ameaças, atuando de forma estratégica para preservar a integridade dos sistemas [Stamp 2005].

Além do mais, o autor deste ensaio reconhece que a ascensão da Inteligência Artificial (IA) tem intensificado tanto as possibilidades quanto os desafios no campo da segurança cibernética. De acordo com Russell & Norvig (2016), a IA vem sendo aplicada em sistemas de detecção automatizada de ameaças, tornando os mecanismos de defesa mais inteligentes e proativos. No entanto, ao mesmo tempo, esses avanços também são explorados por agentes mal-intencionados, que utilizam técnicas de aprendizado de máquina para desenvolver *malwares* mais sofisticados e evasivos.

Já Harari (2018), ao refletir sobre as implicações éticas e sociais das tecnologias emergentes, alerta para a crescente dependência humana de sistemas automatizados, incluindo aqueles voltados à segurança, e para os riscos que surgem quando esses sistemas operam sem supervisão crítica. Nessa perspectiva, o autor reforça que, diante de um cenário em constante transformação, se torna fundamental a presença de profissionais qualificados, capazes de interpretar, intervir e se adaptar continuamente às novas demandas e ameaças trazidas pela evolução tecnológica e pelo uso estratégico da IA.

2.4. Classificação dos Vírus e Suas Ameaças

A evolução da tecnologia da informação, embora tenha proporcionado avanços significativos em diversas áreas, também ampliou o campo de atuação de agentes maliciosos que comprometem a integridade, confidencialidade e disponibilidade dos sistemas computacionais. Dentre essas ameaças, os vírus se destacam por sua diversidade e capacidade de adaptação. Compreender as diferentes classificações desses códigos maliciosos é fundamental para a construção de estratégias de defesa eficazes.

A seguir, serão apresentados os principais tipos de vírus, suas formas de atuação e os riscos que representam ao ambiente digital, com base em estudos e classificações propostas por especialistas e instituições da área de segurança cibernética.

2.4.1. Tipos Comuns de Vírus de Computador

Conforme Stallings (2017), Tanenbaum & Wetherall (2011), Kaspersky (2020a), Symantec (2020), Norton (2021) e Certbr (2021), relacionamos os vírus mais comuns detectados atualmente, os quais podem ser classificados em diferentes categorias, de acordo com seus modos de operação e propagação. A categorização apresentada no Quadro 1 é essencial para o entendimento das ameaças e para a adoção de medidas preventivas e corretivas adequadas:

Quadro 1: Tipo de Vírus Características Principais

Tipo de Vírus	Características Principais
Vírus residente	**Se instala na memória *RAM* do sistema e permanece ativo mesmo após o término de execução do programa inicial. Infecta arquivos continuamente à medida que são acessados, podendo comprometer profundamente o desempenho e a estabilidade do sistema.**
Vírus de ação direta	**Atua de forma rápida e direta, infectando arquivos do tipo *.exe* ou *.com* assim que é executado. Após a infecção, geralmente se *auto deleta*[10], dificultando a detecção e podendo causar danos imediatos ao sistema.**
Vírus *multipartite*	**Combina múltiplas técnicas de infecção, como ataques ao setor de *boot* e arquivos executáveis. Pode se espalhar de diferentes formas simultaneamente, se tornando mais difícil de detectar e remover.**
Sequestrador de navegador (*Browser Hijacker*)	**Modifica configurações do navegador (como página inicial, mecanismo de busca e redirecionamentos de *URL*) sem o consentimento do usuário. Embora classificado como um *malware*, pode coletar dados, exibir propagandas forçadas ou redirecionar para sites perigosos.**
Vírus de substituição	**Apaga ou renomeia arquivos legítimos do sistema, substituindo-os por versões maliciosas ou corrompidas, com aparência semelhante. Pode causar perda irreversível de dados e comprometer a execução de programas críticos.**
Vírus de *script* da *web*	**Escrito em linguagens como *JavaScrip*t ou *VBScript,* esse tipo de vírus se infiltra em sites vulneráveis, sendo ativado durante a navegação. Pode roubar informações, redirecionar links ou instalar outros malwares sem intervenção do usuário.**
Vírus de rede	**Se espalha através de conexões de rede local ou internet, explorando portas abertas, compartilhamentos inseguros e dispositivos vulneráveis. Pode infectar vários computadores em pouco tempo, especialmente em redes corporativas.**
Vírus do setor de inicialização	**Infecta o *MBR*[11] (Master Boot Record) ou o setor de inicialização de mídias como discos rígidos e *pendrives*. Impede a inicialização do sistema operacional e dificulta o uso de ferramentas de recuperação. Exige, em geral, formatação ou ferramentas avançadas para remoção.**

Fonte: Elaborado pelo autor.

[10] Auto deletar ou autoexcluir - significa a ação de algo ou alguém se remover ou excluir a si mesmo. A palavra autoexcluir é um verbo pronominal, indicando que a ação é realizada sobre si próprio. Em alguns ambientes, pode se referir a uma função que apaga dados ou informações automaticamente após um determinado período. Autoexcluir Excluir-se a si mesmo [Priberam 2008-2025].

[11] MBR (*Master Boot Record*) - é um pequeno programa no primeiro setor de um disco rígido ou unidade removível que contém as informações necessárias para iniciar o sistema operacional. Ele identifica onde o sistema operacional está localizado no disco e contém um código que o carrega para a memória *RAM (Randonic Access Memory* ou Memória de Acesso Aleatório) [Tanenbaum 2011; 2015].

Além das características específicas de cada tipo, muitos desses vírus operam como programas inteligentes, capazes de se adaptar ao ambiente em que estão inseridos. Alguns utilizam técnicas avançadas como criptografia, polimorfismo e metamorfismo, permitindo que seus códigos se modifiquem automaticamente a cada infecção. Essa capacidade de *mutação programada* torna a detecção pelos antivírus tradicionais extremamente difícil, exigindo o uso de tecnologias mais sofisticadas de análise comportamental. Esses vírus inteligentes não apenas se camuflam, mas também podem desativar sistemas de segurança, alterar seus próprios rastros e permanecer ocultos por longos períodos, representando uma ameaça contínua, sobretudo em ambientes corporativos e redes interconectadas.

2.4.2. O Que Não é um Vírus: Mitos Comuns

Com o avanço da computação e a crescente digitalização de serviços, surgiram diversas ameaças à segurança da informação. Entre os tipos mais conhecidos estão os *malwares* (abreviação de *malicious software* ou *software* malicioso), que variam em forma e propósito. Para a melhor compreensão de cada uma dessas ameaças, abordaremos a seguir suas ações e características:

- Trojan (Cavalo de Troia ou *Trojan*): É um tipo de *malware* que se disfarça como *software* legítimo para enganar os usuários e induzi-los a instalar programas maliciosos em seus dispositivos. Uma vez instalado, ele pode permitir que cibercriminosos acessem o sistema da vítima, roubem *dados sensíveis*[12] ou instalem outros *malwares*. Diferente de vírus tradicionais, os *Trojans* não se replicam automaticamente, dependendo da ação do usuário para serem ativados [Eset 2025].
- *Worm* (Verme): São programas maliciosos que se replicam automaticamente e se espalham por redes sem a necessidade de interação do usuário. Eles exploram vulnerabilidades em sistemas operacionais ou *softwares* para se propagar, podendo causar lentidão na rede, consumo excessivo de recursos e, em alguns casos, instalação de *backdoors* (ou porta dos fundos) para acesso remoto. Estes se replicam sozinhos e se espalham por redes, causando lentidão e vulnerabilidades [Techtudo 2018].
- *Ransomware*: É um tipo de *malware* que criptografa os dados do usuário ou bloqueia o acesso ao sistema, exigindo o pagamento de um resgate (geralmente em criptomoedas) para restaurar o acesso. Esse tipo de ataque tem se tornado cada vez mais comum, afetando desde usuários individuais até grandes organizações, causando prejuízos financeiros significativos. Sua ação bloqueia o acesso aos arquivos do usuário e exige um pagamento para liberação, sendo uma das formas mais danosas de ataque digital [IBM 2024, Symantec 2021].
- *Rootkit*: São conjuntos de ferramentas que permitem a cibercriminosos obter acesso privilegiado a um sistema e ocultar sua presença. Eles podem modificar o sistema operacional para evitar a detecção por *software*s de segurança, se tornando difíceis de identificar e remover. *Rootkits* podem ser utilizados para espionagem, roubo de dados ou controle remoto do

[12] Dados sensíveis, - conforme a Lei Geral de Proteção de Dados (LGPD), são informações que revelam aspectos mais íntimos e sensíveis da vida de uma pessoa e que, por isso, merecem uma proteção especial. A LGPD define como dados sensíveis aqueles que, se divulgados ou utilizados indevidamente, podem levar a discriminação, preconceito ou violação de direitos fundamentais [Brasil 2018].

sistema comprometido. Por sua vez, visam esconder a presença de invasores no sistema, permitindo acessos não autorizados sem serem detectados [Fortinet 2025].

- *Bugs*[13]: embora não sejam maliciosos, representam falhas de programação ou erro no código de um *software* que causa comportamentos inesperados ou indesejados que podem comprometer o funcionamento e a segurança dos sistemas [Baeldung 2024]. *Bugs* podem resultar de erros de programação, lógica ou *design*, e não são necessariamente maliciosos. Eles podem afetar a funcionalidade, desempenho ou segurança de um sistema, sendo identificados e corrigidos através de processos de teste e depuração. Conhecer essas ameaças é essencial para o desenvolvimento de práticas seguras e conscientes no uso das tecnologias digitais.

Para a detecção e remoção eficaz de ameaças, é indispensável utilizar um programa específico e especializado, devidamente atualizado. Essas ferramentas são projetadas para identificar e neutralizar diversos tipos de ameaças cibernéticas, como vírus, *malware, spyware,* entre outros. A atualização regular desses programas é essencial para garantir que novas ameaças sejam reconhecidas e tratadas adequadamente.

Nos próximos itens, vamos abordar as ferramentas e procedimentos introdutórios necessários para isso. Vamos explorar, de forma introdutória, essas ferramentas para manter a segurança digital efetiva.

2.5. Antivírus e seu Papel na Segurança Digital

Um antivírus é um *software* projetado para detectar, prevenir e remover vírus de dispositivos eletrônicos, como computadores, *PCs, smartphones* e *tablets*. Os antivírus surgiram como resposta à crescente ameaça dos primeiros vírus de computador, que começaram a se disseminar no início da década de 1980.

Em 1987, o pesquisador Bernd Fix desenvolveu o que é considerado o primeiro programa para neutralizar um vírus de computador, o Vienna, dando origem ao conceito de *software* antivírus [Skoudis & Zeltser 2003]. No mesmo ano, surgiram também os primeiros antivírus comerciais na Europa Oriental, como o *Virus* Buster e o AntiVir, este último criado na Alemanha.

As primeiras empresas especializadas em segurança digital começaram a se estabelecer no final dos anos 1980 e início dos 1990, incluindo:

- McAfee (fundada por John McAfee em 1987, nos EUA),
- Symantec (com o famoso Norton Antivírus, lançado em 1991),
- Trend Micro (fundada em 1988, no Japão/EUA),
- Avast *Software* (fundada em 1988, na Tchecoslováquia),
- Kaspersky *Lab* (fundada em 1997, na Rússia).

Essas empresas passaram a desenvolver soluções mais robustas à medida que novas ameaças (*e.g., worms, trojans, spyware* e *ransomwares)m* foram surgindo. Atualmente, o mercado de antivírus conta com uma diversidade de soluções, tanto

[13] *Bugs* - o termo quando usado em um ambiente informatizado, significa erros ou falhas em *software* ou *hardware*. Em tecnologia, erros em sistemas e aparelhos eletrônicos recebem diversas designações, dentre elas: falha, defeito no programa, defeito no *software, bug, tilt* e *glitch* [Wiki, 2023; Tanenbaum 2015].

gratuitas quanto pagas, com empresas como Bitdefender, AVG, ESET, Panda Security, Sophos e Windows Defender (Microsoft), oferecendo proteção integrada ou opcional a usuários domésticos e corporativos [Olhar Digital 2025].

Com o passar do tempo, os antivírus evoluíram de simples varredores de arquivos infectados para sistemas completos de segurança que operam em tempo real, usando inteligência artificial, aprendizado de máquina e análise comportamental para prevenir ameaças ainda não catalogadas [Schneier 1996].

A segurança digital não depende exclusivamente de *softwares* antivírus, mas também da atuação consciente dos usuários de dispositivos inteligentes como microcomputadores, *smartphones* e *tablets*. Segundo Mitnick (1963/2003), o fator humano representa a maior vulnerabilidade nos sistemas de segurança, sendo frequentemente explorado por ataques de engenharia social. Assim, práticas como evitar cliques em *links* suspeitos, manter sistemas atualizados e utilizar senhas fortes se tornam fundamentais. A cultura de prevenção e responsabilidade digital é, portanto, indispensável para a eficácia das ferramentas de proteção.

3. Revisão de Literatura

A origem teórica dos vírus de computador remonta a 1949, quando o cientista John von Neumann, em uma de suas palestras, discutiu a possibilidade de programas se autorreplicarem, cujo conceito foi inspirado no comportamento dos vírus biológicos. Sua visão antecipava, de forma quase profética, a lógica por trás do que viria a ser chamado de *malware*, embora à época isso permanecesse apenas no campo da teoria, devido às limitações tecnológicas e à pouca difusão da computação [Mayumi & Risa 2024].

Foi somente duas décadas depois, com o surgimento da ARPANET[14] em 1969, que os primeiros experimentos práticos começaram a se tornar viáveis. A ARPANET, projeto militar e científico norte-americano, tornou possível a troca de informações à distância por meio da comutação de pacotes e protocolos de rede, sendo um dos marcos na criação da Internet [Mayumi & Risa 2024].

Apesar de o primeiro vírus amplamente disseminado ter surgido apenas em 1982, a ideia de códigos capazes de se replicar já havia sido experimentada anteriormente. Foi criado em 1971 por Bob Thomas, da empresa *BBN Technologies*[15], o vírus *Creeper,* como um experimento pela rede experimental de computadores, a ARPANET (criada em 1969), precursora da internet, sendo ele:

> "[...] projetado para se mover entre computadores conectados, exibindo a mensagem: 'Eu sou o *creeper*, pegue-me se puder!' Embora não causasse danos [sendo] considerado por muitos o primeiro vírus de computador experimental, pois apresentava a capacidade de autorreplicação e propagação entre sistemas. Em resposta, o programa *Reaper* foi criado para remover o

[14] ARPANET (*Advanced Research Projects Agency Network*) - "[...] Rede da Agência para Projetos de Pesquisa Avançada - foi uma rede de computadores construída em 1969 para transmissão de dados militares sigilosos e interligação dos departamentos de pesquisa nos Estados Unidos, inicialmente financiada pela então Agência de Projetos de Pesquisa Avançada (ARPA, atual DARPA) do Departamento de Defesa dos Estados Unidos [...]" [Matthews 2022 tradução nossa].

[15] A BBN *Technologies (*abreviatuda de *Bolt, Beranek and Newman*) - é uma empresa americana de alta tecnologia que fornece serviços de pesquisa e desenvolvimento, com sede em *Massachusetts, EUA*. Foi criada em 1962 e é responsável por um dos primeiros sistemas de tempo compartilhado [BBN 2008; Wiki 2024a].

> *Creeper*, sendo por isso considerado o primeiro 'antivírus' da história [...]" [Thomas 2023 tradução nossa].

Apesar de teorias anteriores, como a de John von Neumann em 1949, que já discutia a possibilidade de programas autorreplicantes[16], a ausência de computadores acessíveis e redes integradas impediu que tais ideias fossem testadas na prática por décadas. Somente com a popularização dos computadores pessoais no início da década de 1980, especialmente modelos como o *Apple* II, foi possível observar os primeiros casos reais de infecção digital [Mayumi & Risa 2024].

O *Elk Cloner* criado em 1982 por Rich Skrenta, então com 15 anos, como uma brincadeira que infectava disquetes do *Apple* II [Denning 1990]. Ele se replicava automaticamente ao ser inserido em outros computadores, introduzindo um conceito inédito para a época: a autorreplicação de código malicioso. "Mesmo com o *Creeper* (meados de 1971) vindo antes, o *Elk Cloner* (em 1982) é considerado como o primeiro vírus de contaminação em massa" [Mathias 2024, Matthews 2022].

Em 1986, surgiu o *Brain*, primeiro vírus conhecido para computadores IBM PC com *MS-DOS*[17]. Criado por dois irmãos paquistaneses, Basit e Amjad Alvi, seu objetivo inicial era proteger um *software* contra cópias ilegais, mas acabou se espalhando mundialmente por meio de disquetes 5¼ polegadas [Spafford 1994, Ludwig 1998]. Esses primeiros vírus não tinham fins destrutivos, mas abriram caminho para usos cada vez mais danosos e complexos da tecnologia. O intuito original dos criadores era proteger um *software* médico de sua autoria contra cópias não autorizadas, funcionando como uma forma rudimentar de controle de direitos autorais no ambiente digital [Wiki 2024b].

Com a expansão da internet na década de 1990, os vírus se multiplicaram em escala global. Se tornaram comuns por meio de anexos de *e-mail*, *downloads* de programas piratas, sites infectados e pen drives comprometidos. Um exemplo marcante foi o *ILOVEYOU* (traduzido para o português: *EUTEAMO*), disseminado por *e-mail* em 2000, que causou prejuízos bilionários ao enganar usuários com uma falsa mensagem amorosa [Certbr 2201, BBCNews 2000].

Nas décadas seguintes, os vírus evoluíram de simples brincadeiras para ameaças sofisticadas. Muitos operam hoje de forma furtiva, voltados ao roubo de dados, espionagem corporativa, ataques coordenados ou extorsão por meio de *ransomware* [Symantec 2021]. A atuação de grupos organizados transformou os vírus em armas digitais com impacto econômico e político significativo.

Atualmente, os vírus de computador fazem parte de uma categoria maior chamada *malwar*e, que inclui outras ameaças como *worms, trojans* e *ransomwares*. A principal característica dos vírus é a autorreplicação e a necessidade, na maioria dos casos, de uma ação do usuário para ativação, como exemplo: clicar em anexos ou *links* maliciosos [Stallings 2019, Kaspersky 2020a, LinkNacional 2022]. Muitos se escondem em arquivos aparentemente inofensivos, como *PDF*s, imagens e vídeos.

---

[16] Programas autorreplicantes - são códigos maliciosos que se multiplicam automaticamente (que fazem autorreplicação), podendo causar lentidão, falhas no sistema ou roubo de dados, e exigem ferramentas especializadas para sua detecção e remoção [Stamp 2005].

[17] MS-DOS (acrônimo para *Microsoft Disk Operating System*) - foi um sistema operacional amplamente utilizado em computadores pessoais IBM-PC e compatíveis durante a década de 1980 e início dos anos 1990. Era um sistema operacional de linha de comando, o que significava que os usuários interagiam com o computador através de comandos digitados no teclado [Tanenbaum 2011; 2015].

Outrossim, existem os chamados vírus adormecidos, que permanecem inativos até que um evento específico os ative, agindo em segundo plano sem que o usuário perceba. Roteadores de redes públicas (*e.g.,* cafés, *lan houses* e aeroportos), também se tornaram alvos vulneráveis: podem ser alterados ou infectados para capturar dados sensíveis ou redirecionar acessos para sites falsos [Kaspersky 2020a, Norton 2021].

Conforme o Canaltech, em sua publicação sobre o boletim da Kaspersky de 2020, afirmou que :

> "[...] não foi apenas o novo coronavírus (SARS-CoV-2) que se replicou ao redor do mundo ao longo dos últimos meses. Segundo a companhia, só neste ano, foram criados cerca de 360 mil novos vírus para computadores e *smartphones* por dia - se fizermos uma conta rápida levando em consideração 365 dias, estamos falando de um total de 131,4 milhões de ameaças [...]" [Souza 2020b].

Entre novembro de 2019 e outubro de 2020, a *Kaspersky* analisou dados de milhões de usuários ao redor do mundo, que permitiram o monitoramento de ameaças digitais por meio da rede *Kaspersky Security Network* (KSN). Nesse período, 10,18% dos computadores conectados à internet sofreram ao menos um ataque de *malware* [Kaspersky 2020b tradução nossa].

As soluções da *Kaspersky* bloquearam mais de 666 milhões de ataques *online*, identificaram 173 milhões de links maliciosos e mais de 33 milhões de objetos nocivos. Foram registradas também 549 mil tentativas de *ransomware*, 1,5 milhão de ataques por mineradores ilegais de criptomoedas e 668 mil tentativas de roubo de dinheiro via acesso a contas bancárias *online* [Kaspersky 2020b tradução nossa]. Esses dados mostram a intensidade das ameaças virtuais e a importância da proteção digital constante.

Por essa razão, a literatura enfatiza a importância da prevenção. Medidas como o uso de antivírus atualizados, boas práticas de navegação, não clicar em *links* desconhecidos e evitar o uso de mídias removíveis sem escaneamento prévio são fundamentais [Denning 1990, Stallings 2019]. A segurança digital se tornou uma das áreas mais estratégicas da computação, exigindo conhecimento técnico e consciência crítica dos usuários [Anderson 2008].

3.1. Métodos de Disseminação de Ameaças

As ameaças digitais utilizam diferentes métodos para se disseminar entre sistemas e redes, explorando vulnerabilidades técnicas e comportamentais dos usuários. A compreensão dessas estratégias é essencial para o desenvolvimento de mecanismos eficazes de prevenção e resposta. Nesta seção, abordamos os principais vetores de propagação utilizados por códigos maliciosos no ambiente computacional.

3.1.1. Vírus e *Malware*

Malware, como vírus, *worms*, *trojans* e *ransomwares*, são códigos maliciosos que comprometem sistemas operacionais, corrompem arquivos e possibilitam acessos remotos não autorizados [Skoudis & Zeltser 2003, Paloalto 2025]. *Hackers* maliciosos costumam utilizar essas ferramentas para:

- Roubar dados sensíveis;

- Instalar *backdoors*[18];
- Minerar criptomoedas;
- Criar *botnets*[19] para ataques distribuídos (ou ataques *DDoS*[20]).

A disseminação de vírus pode ocorrer por:

- Anexos de *e-mail* contaminados;
- Dispositivos USB infectados;
- Download de *softwares* falsos;
- Vulnerabilidades em navegadores e *plugins*[21].

Além dos computadores, os *smartphones* (aparelhos celulares) também passaram a integrar o cenário das ameaças cibernéticas de maneira intensa, e a conscientização dos usuários sobre os riscos de infecção é essencial.

A implementação de medidas preventivas, como evitar aplicativos de fontes duvidosas, manter o sistema atualizado e utilizar soluções de segurança, pode contribuir para ambientes digitais mais seguros. A alfabetização digital e o acesso à informação confiável são os principais aliados da sociedade na prevenção contra vírus e outros *malwares*.

A evolução dos vírus de computador acompanha diretamente o avanço dos sistemas computacionais, das redes e da própria internet. Desde as primeiras décadas da computação pessoal, os códigos maliciosos passaram de experimentos acadêmicos e programas simples autorreplicantes para ameaças complexas, capazes de se propagar em larga escala, explorar vulnerabilidades sofisticadas e causar impactos significativos à segurança da informação, à privacidade e à continuidade dos sistemas. Ao longo do tempo, o crescimento exponencial do número de malwares esteve associado ao aumento da conectividade global, à popularização dos sistemas operacionais e ao surgimento de novos vetores de ataque, como redes corporativas, dispositivos móveis e ambientes em nuvem [Tanenbaum 2011, Cohen 1987, Stamp 2005, Stallings 2019].

A Figura 1 apresentada a seguir, sintetiza essa evolução histórica, evidenciando marcos temporais, o aumento aproximado da quantidade de vírus e a sofisticação progressiva das técnicas empregadas. As informações foram consolidadas a partir de literatura clássica e contemporânea da área de Segurança da Informação e Sistemas Operacionais, bem como de relatórios técnicos de empresas especializadas em cibersegurança, como IBM (2025) e Kaspersky (2020a, 2020b), garantindo fundamentação teórica e atualização conceitual.

---

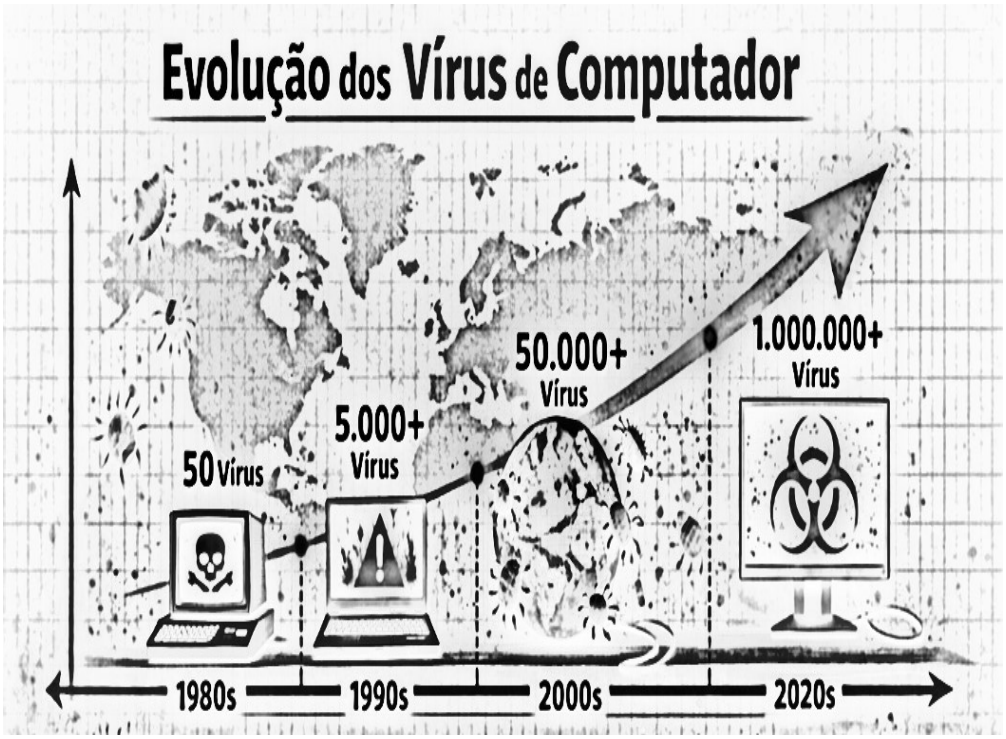
[18] *Backdoor* - também conhecido como *porta dos fundos* —é uma forma de acesso, geralmente não autorizada, a um sistema, *software* ou rede, que contorna as medidas de segurança convencionais. É um método utilizado por cibercriminosos para obter acesso contínuo e oculto, permitindo-lhes controlar o sistema, roubar dados, instalar mais *malware* ou causar danos <https://pt.wikipedia.org/wiki/Backdoor>.

[19] *Botnet* - é uma rede de computadores, dispositivos Internet das Coisas (IoT) e outros dispositivos, infectados com *malware* e controlados por um indivíduo (o *botmaster*), que os usa para realizar atividades maliciosas em larga escala, como ataques *DDoS*, *spam*, roubo de dados, entre outros [Skoudis & Zeltser 2003, Paloalto 2025].

[20] *DDoS* (*Distributed Denial-of-Service*) - é um tipo de ataque cibernético que visa sobrecarregar um sistema, serviço ou rede com uma quantidade massiva de tráfego, tornando-o indisponível para usuários legítimos. Ao contrário de um ataque *DoS* (*Denial-of-Service*) que utiliza um único ponto de ataque, o *DDoS* usa uma rede de dispositivos (*botnets*) para coordenar o ataque [Skoudis & Zeltser 2003].

[21] *Plugin (*em informática) - é um programa de computador que estende as funcionalidades de outro programa. É uma extensão que adiciona funcionalidades específicas, como ferramentas de edição de imagem, leitores de vídeo ou até mesmo suporte a novos tipos de ficheiros [Stamp 2005].

Figura 1 – Evolução dos vírus de computador ao longo do tempo



Fonte: Elaborado pelo autor baseado em IBM (2025) e Kaspersky (2020a, 2020b).

A partir de 2020, observa-se um novo salto evolutivo no ecossistema de malwares, impulsionado pelo aumento significativo das velocidades de conexão e pela ampliação da superfície digital. A transição de conexões discadas e via rádio para conexões de alta velocidade, como a fibra óptica nos domicílios, reduziu drasticamente o tempo de propagação de códigos maliciosos, potencializando sua disseminação em escala global (Stamp 2005, Stallings 2019). Esse cenário é agravado pela ampla utilização de dispositivos móveis (*e,g,,* celulares, tablets e notebooks) conectados de forma contínua e distribuídos em diferentes ambientes de rede, bem como pela intensificação do uso de redes sociais e de técnicas de engenharia social, que exploram o fator humano como vetor primário de infecção [IBM 2025, Kaspersky 2020a, Norton 2021].

A falta de limitação no uso dos sistemas, aliada à imperícia dos usuários decorrente da insuficiência de conhecimento técnico, mesmo diante da existência de orientações e boas práticas amplamente divulgadas, contribui significativamente para a elevação dos riscos. Tal contexto corrobora as análises de Mitnick & Simon (2003), ao evidenciar que, apesar da evolução tecnológica e da sofisticação dos mecanismos de defesa, o elo mais vulnerável da segurança da informação permanece sendo o fator humano.

Nos próximos itens, abordaremos especificamente as vulnerabilidades dos celulares e os riscos a que esses dispositivos estão expostos.

3.2. Celulares e a Vulnerabilidade a Vírus

Durante muito tempo, os vírus digitais eram uma preocupação restrita aos computadores. Com o avanço da tecnologia e a crescente dependência de dispositivos móveis, os *smartphones* se tornaram um dos principais alvos de programas maliciosos. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE) de 2021, "[...] mais de

84% da população brasileira com mais de 10 anos utiliza celular, e em 99,5% dos lares o acesso à internet é feito por meio desses dispositivos. Esse panorama evidencia a centralidade dos celulares na vida digital em nossos dias atuais [...]" [Ibge 2024].

Conforme Universo *Online* (UOL)*,* considerada a maior empresa brasileira de conteúdo, divulga em sua publicação referente ao ano de 2023 que:

> "[...] 163,8 milhões de pessoas tinham aparelho de telefone celular para uso pessoal no País, o equivalente a 87,6% da população com 10 anos ou mais. Os dados são da Pesquisa Nacional por Amostra de Domicílios Contínua – Tecnologia da Informação e Comunicação 2023, a Pnad TIC, e foram divulgados pelo Instituto Brasileiro de Geografia e Estatística [...]" [Uol 2024].

Diante desse cenário, cresce a atuação de cibercriminosos que desenvolvem *malwares* direcionados a esses aparelhos, com foco na obtenção de dados pessoais e financeiros. O sistema *Android*[22] é o mais visado, por representar a maioria dos dispositivos no Brasil e por apresentar uma estrutura de código mais aberto. Ainda assim, usuários de *iOS* não estão isentos de riscos, especialmente quando realizam práticas como o *jailbreak*[23], que fragilizam a segurança do sistema [Ibge 2022, Uol 2021, Kaspersky 2025a].

Conforme Kaspersky (2025b), "[...] embora seja permitida, a aplicação de código de *jailbreak* ao seu telefone não é necessariamente segura. O desbloqueio dá aos cibercriminosos a oportunidade de *hackear* seu telefone", ainda informa como a *Apple* considera o uso do desbloqueio: "[...] considera o *jailbreak* do *iOS* uma violação dos seus termos e condições de uso e avisa os clientes que a prática expõe o telefone a vários riscos [...]", levando até em anulação da garantia dos aparelhos.

Os efeitos da infecção por vírus em celulares são diversos, podendo incluir lentidão do sistema, travamentos, consumo excessivo de dados e bateria, além de espionagem e roubo de informações sensíveis. Existem *malwares* capazes de modificar dados bancários em tempo real, como alterar o destinatário de uma transferência via Pix. Como observa a *University of Houston-Downtown*, e demonstra que a luta contra essas ameaças exige vigilância constante e atualização contínua dos mecanismos de defesa [UHD 2025b].

Os efeitos da infecção por vírus em celulares são diversos, podendo incluir lentidão do sistema, travamentos, consumo excessivo de dados e bateria, além de espionagem e roubo de informações sensíveis. Segundo a Kaspersky (2023), *malwares* móveis podem acessar dados pessoais, interceptar mensagens, realizar chamadas não autorizadas e até modificar informações financeiras em tempo real. Conforme aplicativo *Pic`Pay,* cujos aplicativo atuam como uma carteira digital e banco digital, ele orienta em sua publicação que: "[...] existe um *malware* que é capaz de alterar os dados do destinatário de um Pix no momento da transação. Isso mostra a importância de aprender a identificar se o seu *smartphone* está com algum vírus [...]". Além dos pagamentos via PIX, inclui também as transações bancárias, colocando em risco a segurança financeira dos usuários [Picpay 2023].

---

[22] *Android* - é utilizado em uma grande variedade de dispositivos, incluindo *smartphones, tablets, smart* TVs, relógios inteligentes (smartwatches -*Wear OS*), carros (*Android Auto*), e em alguns *consoles* de *videogame,* câmeras digitais, e outros dispositivos eletrônicos [https://pt.wikipedia.org/wiki/Android].

[23] *Jailbreak* (em português *quebra de segurança*) - é um processo que permite a usuários de dispositivos *Apple* (*e.g.,* aparelhos *iPhones* e *iPads*) - obter acesso à raiz do sistema operacional *iOS*. Isso dá acesso a recursos e funcionalidades que a *Apple* normalmente não permite ou que estão disponíveis apenas através de métodos não oficiais [Ibge 2021, Uol 2021, Kaspersky 2025a].

Outrossim, *ibidem* orienta que a detecção de vírus pode ser feita por meio da observação de sinais como aumento no consumo de internet, superaquecimento do aparelho, surgimento de anúncios indesejados, aplicativos desconhecidos ou ações não reconhecidas pelo usuário, como envios de mensagens ou *e-mails* automáticos. Esses sintomas indicam que o dispositivo pode estar executando tarefas em segundo plano, comuns a *softwares* maliciosos. A utilização de ferramentas antivírus, aliada a práticas seguras de uso digital, é essencial para garantir a integridade do dispositivo [Picpay 2023].

3.3. Engenharia Social

A engenharia social é uma técnica não técnica, mas extremamente eficaz, que visa explorar a confiança ou ignorância dos usuários para obter acesso a informações confidenciais [Mitnick & Simon 2002]. As técnicas mais comuns incluem:

- *Phishing:* envio de mensagens falsas que simulam entidades confiáveis;
- *Pretexting*: fingir ser alguém com autoridade para obter dados;
- *Baiting:* uso de mídias infectadas deixadas propositalmente em locais públicos;
- *Tailgating*: acesso físico forçado por meio de engano.

Essas práticas mostram que a segurança não depende apenas de sistemas bem configurados, mas também da conscientização e treinamento dos usuários**.**

O autor, em seu outro estudo sobre *Crimes Cibernéticos*, conceitua a engenharia social como sendo: "[...] uma técnica não necessariamente técnica, mas extremamente eficaz: consiste na manipulação psicológica de usuários para obter dados sensíveis ou acesso indevido a sistemas [...]" [Brandão 2025 p. 3].

Além do que já foi exposto, é essencial conhecer outros métodos de detecção. Com a crescente complexidade das ameaças cibernéticas, práticas como *Ethical Hacking* e *Penetration Tests* tornam-se essenciais para identificar vulnerabilidades antes que sejam exploradas. Essas simulações de ataques reais, com fins preventivos, fortalecem a segurança digital. Compreender como as ameaças se disseminam é, portanto, fundamental para orientar ações eficazes de proteção. Abordaremos esses aspectos nos próximos itens.

3.4. *Ethical Hacking, Penetration Testing* e os Métodos de Disseminação de Ameaças

Diante da crescente complexidade das ameaças cibernéticas, práticas como o *Ethica*l *Hacking* e os *Penetration Tests* se tornaram essenciais para identificar vulnerabilidades antes que sejam exploradas por agentes maliciosos. Essas abordagens simulam ataques reais com fins preventivos e educativos, contribuindo para o fortalecimento da segurança digital. Nessa perspectiva, compreender os métodos de disseminação de ameaças é fundamental para orientar ações proativas e eficazes na proteção de sistemas e redes.

3.4.1. *Ethical Hacking* e sua Finalidade

O *ethical hacking* é uma prática essencial no campo da cibersegurança, em que profissionais autorizados, conhecidos como *hackers éticos*, simulam ataques cibernéticos com o objetivo de identificar vulnerabilidades e falhas em sistemas

computacionais antes que sejam exploradas por criminosos reais [Baloch 2015 p. 121-125].

Nessa abordagem, o hacker ético reproduz com precisão as técnicas utilizadas por agentes maliciosos (*black hats*[24]), incluindo invasões de rede, ataques via *malware* e exploração de falhas conhecidas [Kim & Soloman 2016]. Isso permite testar a capacidade de resistência da organização diante de diferentes cenários de ataque, proporcionando uma visão realista da maturidade em segurança da informação.

O autor, como especialista em segurança cibernética, esclarece que as regras de segurança da informação e cibernética, em geral, incluem a proteção contra ameaças internas e externas, a prevenção de perdas e danos, a garantia de disponibilidade dos recursos e a manutenção da confidencialidade, integridade e autenticidade das informações

O processo geralmente envolve:

- Coleta de informações (reconhecimento);
- Escaneamento de vulnerabilidades;
- Geração de *payloads*[25] simulados;
- Testes de acesso e *exfiltração simulada de dados*[26].

Essas ações seguem protocolos de segurança da chamada *Cyber Security Ethical Hacking* (em português, Segurança cibernética *Hacking* ético**),** que prioriza a ética, a confidencialidade e a legalidade do processo [EC-Council 2023].

Conforme Okpa *et al*. (2022), sobre as organizações corporativa e posturas a serem adotadas, sobre os *firewalls*[27], os autores afirmam que:

> "[...] devem fortalecer seus *firewalls* e educar seus funcionários sobre os perigos de visitar sites inseguros e baixar anexos não verificados ou clicar em *links* em *e-mails* desconhecidos. Grandes corporações devem contratar especialistas em segurança de TIC para realizar um teste de penetração em sua rede, com a intenção de identificar quais vulnerabilidades existem e realizar as reparações necessárias para prevenir possíveis formas de ataque ou violação [...]" [Okpa *et al*. 2022 p. 9 tradução nossa].

[24] *Black hat* (chapéu preto) - se refere a um *hacker* ou *cracker* que viola leis ou padrões éticos para fins nefastos, como crimes cibernéticos ou malícia. São frequentemente considerados como criminosos cibernéticos que exploram vulnerabilidades de *softwares* ou sistemas corporativos para fins de ganho financeiro, roubo de dados ou outras atividades ilegais [Kim & Soloman 2016].

[25] *Payload* (em português, *carga útil*) - se refere à parte dos dados transmitidos que é a mensagem principal ou informação que está a ser transferida. No ambiente computacional e das redes de computadores, sendo a parte dos dados que, essencialmente, contém a informação relevante, como um ficheiro, um pedido de serviço ou um comando. [https://pt.wikipedia.org/wiki/ Carga_útil_(computação)].

[26] Exfiltração simulada de dados (também conhecida como exfiltração de dados de teste) - é uma técnica utilizada em segurança cibernética para simular a exfiltração (roubo de dados) real de dados confidenciais de um sistema ou rede. Esta simulação permite às organizações identificarem vulnerabilidades na sua segurança, avaliar a eficácia dos seus mecanismos de proteção e treinar a sua equipa para responder a ataques de exfiltração [Wack & Tracy 2003].

[27] *Firewall* - é um sistema de segurança que controla o tráfego de rede, permitindo ou bloqueando conexões com base em um conjunto de regras. Ele funciona como um guarda de segurança na porta, verificando o que entra e sai da rede, protegendo contra acesso não autorizado, vírus, *malware* e outros riscos [Okpa *et al.* 2022].

3.4.2. *Pentesting*[28]: Uma Abordagem Controlada

O *penetration testing* ou *pentest* - difere do *ethical hacking* por sua abordagem mais estruturada e delimitada. Neste caso, a empresa contratante define previamente os escopos de teste, ou seja, o objetivo que se pretende atingir, como quais servidores, sistemas ou redes devem ser analisados. A equipe de *pentest* executa ações específicas de invasão simulada e, ao final, apresenta um relatório com métricas técnicas, nível de exposição, vulnerabilidades encontradas e sugestões de mitigação [Andress 2014].

O Relatório de *Pentest* é um documento essencial que certifica que todas as ações realizadas ocorreram conforme os acordos contratuais e legais, e serve como base para planos de ação em segurança da informação.

3.4.3. Legalidade e Ética do *Ethical Hacking*

É fundamental destacar que o *ethical hacking* não é ilegal**,** desde que contratado e autorizado pela organização alvo [Okpa *et al.* 2022]. Para ser considerado ético e legal, esse tipo de serviço deve respeitar três premissas principais:

i. Ser autorizado formalmente pela empresa;

ii. Não comprometer as operações da organização;

iii. Atuar em conformidade com legislações, como a Lei Geral de Proteção de Dados (LGPD), ref. Lei 13.709/18 [Brasil 2018]. Outrossim, o hacker ético não pode**:**

- Usar *softwares* piratas;
- Divulgar dados sensíveis;
- Atuar para empresas não contratantes;
- Violar normas legais ou éticas [EC-Council 2023; Wiki 2025a, 2025b].

3.4.4. Classificação dos Tipos de *Hackers*

A comunidade *hacker* é dividida em três principais perfis [Kapoor 2018]:

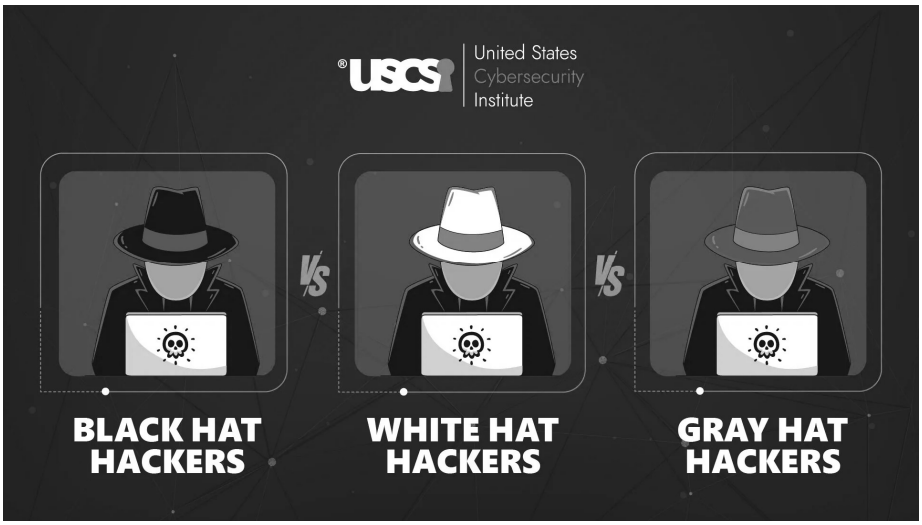
- *White hat* (Chapéu branco): os *hackers* éticos, que trabalham para proteger sistemas;
- *Black hat* (Chapéu preto)**:** *hackers* mal-intencionados que exploram vulnerabilidades com fins ilícitos;
- *Gray hat* (Chapéu cinza): uma categoria intermediária que explora falhas, mas sem intenção clara de prejudicar ou ajudar.

Além dos agentes que atuam na proteção de sistemas, existem indivíduos que empregam seus conhecimentos técnicos com finalidades maliciosas, como o roubo de dados, sabotagem digital e disseminação de códigos maliciosos. Esses agentes são tecnicamente classificados como *crackers,* se diferenciando dos *hackers* éticos por sua intenção deliberada de causar danos ou obter vantagens ilícitas. A Figura 2 ilustra representações comuns atribuídas aos diferentes perfis de *hackers*, frequentemente

[28] *Pentest, penetration testing* ou *pentesting* - se referem a um teste de segurança que simula um ataque cibernético para identificar e avaliar as vulnerabilidades de um sistema, rede ou aplicação. A intenção é encontrar falhas de segurança que um *hacker* malicioso poderia explorar, permitindo que a empresa tome medidas corretivas antes que um ataque real ocorra [Baloch 2015 p. 121-125].

observadas em materiais de divulgação, campanhas educativas ou análises técnicas relacionadas a ataques cibernéticos, conforme descrito anteriormente.

Figura 2: Compreendendo a diferença entre hackers Black, White e Gray-Hat



Conforme Silva (2025), o termo *hacker* é frequentemente associado, no senso comum, como uma figura obscura. Embora filmes e séries muitas vezes retratem hackers como figuras obscuras dominando sistemas com facilidade, essa imagem é glamourizada e distorcida; na realidade, ataques cibernéticos são complexos, envolvem muitas etapas de reconhecimento e exploração e estão muito mais ligados a roubo de dados, fraude e danos econômicos do que a "sistemas de ponta" em si.

Essa romantização pode confundir a percepção pública sobre o tema. No entanto, essa representação é bastante distorcida da realidade. A prática do *hacking,* na sua essência, envolve um processo técnico, complexo e sofisticado, que demanda elevado conhecimento em redes, sistemas operacionais, linguagens de programação e arquitetura de sistemas. Longe do glamour fictício, o *hacking* (especialmente em sua vertente ética), está voltado à identificação de vulnerabilidades com o objetivo de fortalecer a segurança cibernética, sendo um campo de estudo e atuação essencial na era da informação [Silva 2025].

4. Metodologia

Este estudo se caracteriza como uma pesquisa exploratória com base em levantamento bibliográfico e análise de documentos técnicos, como manuais de segurança digital, relatórios de empresas de cibersegurança e artigos divulgados por especialistas da área. Os dados foram organizados em categorias temáticas para facilitar a compreensão dos fenômenos analisados. Uma pesquisa de abordagem qualitativa e exploratória, com foco na sistematização teórica de conceitos relacionados à ameaça e segurança digital. A construção do texto se baseou em levantamento bibliográfico, com recorte de tempo dos últimos 20 anos, totalizando a análise de 105 fontes entre artigos científicos, livros técnicos, normas e publicações institucionais sobre tecnologia da informação.

A seleção dos materiais seguiu critérios de relevância temática e atualidade, priorizando publicações que tratassem da evolução dos vírus de computador, suas formas de disseminação, prevenção e impacto nos sistemas. Para o refinamento da pesquisa, foram utilizados os seguintes descritores: Vírus de computador, *malware*, segurança cibernética, infecção digital, antivírus, ameaças digitais e engenharia social.

O estudo ainda incorporou reflexões oriundas da experiência prática do autor, atuante no setor de Tecnologia da Informação e segurança cibernética, o que contribuiu para a contextualização crítica do fenômeno abordado. A opção por um ensaio teórico-introdutório impôs, contudo, certas limitações, como a ausência de estudos de caso empíricos e a não abordagem aprofundada de aspectos técnicos de programação e codificação de *malwares* avançados.

5. Discussão

Com o avanço da tecnologia e a ampliação do acesso à internet, a proliferação de vírus e outros tipos de *malwares* se tornou uma das maiores preocupações no campo da segurança digital. Vírus de computador são programas maliciosos capazes de se replicar e se propagar por arquivos e sistemas, afetando o desempenho, a segurança e a integridade de dados. Inicialmente disseminados por disquetes, hoje se espalham por *e-mails*, *downloads* suspeitos, redes e dispositivos USB. Outrossim, estratégias como a engenharia social que explora emoções humanas como medo, urgência e curiosidade, têm sido amplamente utilizadas por *hackers* para burlar o senso crítico dos usuários e obter acesso indevido a sistemas e informações.

A detecção de infecções por vírus nem sempre é simples, visto que muitos desses códigos maliciosos operam de forma silenciosa, camuflando sua presença enquanto comprometem sistemas. Isso demanda ferramentas específicas de proteção e atuação de profissionais qualificados. Entre os tipos mais comuns de ameaças estão os *trojans*, *worms, ransomwares* e *rootkits*, cada um com mecanismos próprios de ataque e propagação. Paralelamente, a ascensão da inteligência artificial tem tanto potencializado os sistemas de defesa quanto ampliado a sofisticação dos ataques. Assim, diante de um cenário digital cada vez mais complexo, se torna essencial investir não apenas em tecnologia, mas também em conhecimento técnico e educação digital para mitigar riscos e preservar a segurança da informação.

A discussão em torno da evolução dos vírus de computador revela um fio condutor entre a teoria inicial de John von Neumann (1949) e os desenvolvimentos práticos que se seguiram a partir da década de 1970, conforme apontado por Mayumi & Risa (2024). Os autores destacam que, embora von Neumann tenha proposto o conceito de programas autorreplicantes, foi apenas com o advento da ARPANET e o experimento de Bob Thomas com o vírus *Creeper* em 1971 que essas ideias ganharam materialidade [Matthews 2022].

Denning (1990) e Spafford (1994) corroboram essa linha de desenvolvimento ao relacionar o surgimento do *Elk Cloner* e do *Brain* com o cenário da popularização dos computadores pessoais e da proliferação do sistema MS-DOS, estabelecendo a transição de experimentos inofensivos para ameaças com alcance global. A partir da década de 1990, autores como BBCNews (2000), Certbr (2021) e Symantec (2021) descrevem a escalada de complexidade e sofisticação dos vírus, os quais passaram a ser usados em campanhas de engenharia maliciosa, espionagem e cibercrime em larga escala.

No que se refere à disseminação das ameaças, Stallings (2019), Kaspersky (2020a), Norton (2021) e Souza (2020b) descrevem a diversidade de métodos utilizados, que incluem desde anexos contaminados e mídias removíveis até roteadores públicos comprometidos. Mitnick & Simon (2002; 1963/2003) e Brandão (2025) acrescentam a esse debate a relevância da engenharia social como estratégia não técnica, mas eficaz, de manipulação de usuários para obtenção de dados sensíveis.

A convergência entre esses autores mostra que, além de falhas tecnológicas, as vulnerabilidades humanas seguem sendo exploradas com frequência, exigindo abordagens integradas de segurança. Neste sentido, a literatura evidencia a importância de práticas preventivas, como as defendidas por Anderson (2008) e pela Kaspersky (2020b) e outros autores, que sustentam a necessidade de treinamento contínuo de usuários e atualização constante de sistemas de proteção.

Apesar dos avanços tecnológicos, como o uso de inteligência artificial em antivírus [SCHNEIER 1996], a eficácia da segurança digital ainda depende do comportamento do usuário. Mitnick (2002) aponta o ser humano como o elo mais frágil, alvo frequente de engenharia social. Assim, é essencial adotar práticas seguras no uso de dispositivos. Ainda corroborando nessa linha de pensando, Skoudis & Zeltser (2003), afirma que a proteção eficaz resulta da combinação entre tecnologia e conscientização do usuário.

Dessa forma, autores como Baloch (2015), Kim & Soloman (2016) e Okpa *et al*. (2022) reforçam a necessidade do *ethical hacking* e dos *penetration tests* como mecanismos legítimos de antecipação de ameaças. A prática de simular ataques, conforme defendem esses estudiosos, proporciona uma resposta proativa às ameaças descritas por Kaspersky (2020b) e Symantec (2021), se alinhando com a urgência apontada por Souza (2020b) diante da escala diária de novos *malwares*. Esses procedimentos permitem não apenas avaliar a resiliência de sistemas, mas também alinhar as políticas corporativas de segurança às exigências de um ambiente digital em constante mutação.

6. Conclusão

A compreensão sobre os vírus de computador se revela fundamental para a promoção da segurança digital no uso cotidiano e profissional da tecnologia. Ao longo deste ensaio, se buscou responder às questões centrais propostas e alcançar os objetivos estabelecidos, como esclarecer o que é um vírus de computador, suas classificações, comportamentos, formas de contágio e disseminação, além de abordar a atuação de *hackers* e aspectos de engenharia social. A análise demonstrou que, com o avanço tecnológico, os vírus se tornaram mais sofisticados, incorporando recursos de inteligência artificial e algoritmos autoadaptativos, que lhes conferem maior autonomia, adaptabilidade e capacidade de evasão dos sistemas de defesa tradicionais.

Além disso, foi possível compreender que infecções em larga escala comprometem não apenas a integridade de dados e o funcionamento de sistemas, mas também provocam sérios danos econômicos e abalam a confiança social em infraestruturas críticas, sobretudo nos setores público e corporativo. O estudo também abordou os principais tipos de vírus, seus modos de infecção e as estratégias preventivas mais eficazes, reforçando a importância de práticas seguras, como a utilização de *softwares* antivírus confiáveis, atualização constante dos sistemas e a promoção de uma educação digital crítica e acessível a todos os perfis de usuários. Se Ressaltou, ainda, a relevância de medidas proativas, como o *ethical hacking* e os testes de penetração, para identificar vulnerabilidades antes que sejam exploradas por agentes maliciosos.

Contudo, algumas limitações foram identificadas. Por se tratar de um ensaio introdutório e generalista, não foi possível aprofundar aspectos técnicos como a

engenharia reversa de códigos maliciosos, a atuação de *malwares* em ambientes corporativos ou os impactos específicos em dispositivos móveis. Tampouco foram apresentados dados empíricos atualizados ou estudos de caso práticos que pudessem ilustrar com mais precisão a magnitude dos ataques em diferentes setores.

Diante dessas limitações, propõem-se as seguintes questões para futuras investigações: De que maneira os vírus baseados em inteligência artificial estão desafiando os modelos tradicionais de detecção e resposta em cibersegurança? E quais políticas públicas, estratégias institucionais e ações educacionais (tanto no âmbito da educação acadêmica quanto da conscientização da população em geral), podem ser implementadas para mitigar os impactos econômicos e sociais causados por ciberataques em setores críticos, como saúde, educação e energia? Ressalta-se que tais questões não encontram resposta direta neste texto, mas visam estimular reflexões e pesquisas aprofundadas sobre os caminhos possíveis para o enfrentamento dos desafios atuais da segurança digital.

Referências

ANDERSON, R. (2008). ***Security engineering***: *a guide to building dependable distributed systems*. Idioma ingles. 2. ed. *Indianapolis: Wiley*, 1080 p. Disponível em: <https://www.cl.cam.ac.uk/~rja14/book.html>. Acesso em: 02 jun. 2025.

ANDRESS, J. ***The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice***. Idioma ingles. ISBN:978-0128007440, [s.l.]: Syngress Publishing, jun. 2014, 240 p.

BAELDUNG (2024). ***Bugs and Debugging in Programming*.** [*online*]. [s.l.]: *Baeldung*, [n.p.]. Disponível em: <https://www.baeldung.com/cs/bugs-debugging>. Acesso em: 29 maio 2025.

BALOCH, R. (2015) ***Ethical Hacking and Penetration Testing Guide*.** [*online*] *Pdf*. Idioma ingles. *Boca Raton, Flórida: CRC Press*, 41 p. Disponível em: <https://tsoungui.fr/ebooks/Ethickal-haking-postexploitation.pdf>. Acesso em: 02 jun. 2025.

BBCNEWS (2000). ***ILOVEYOU virus attacks millions***. [*online*]. Idioma Ingles. *Londres*: *BBC News,* [n.p.]. Disponível em: <http://news.bbc.co.uk/2/hi/asia-pacific/737478.stm>. Acesso em: 01 jun. 2025.

BBN (2008). ***BBN Technologies and Digital Force Technologies Partner for Growth***. [*online*], Idioma ingles. San Diego, CA: Digital Force, June 24, 2008, [n.p.]. Disponível em: <ttps://web.archive.org/web/20121225105913/http://www.digitalforcetech.com/news.html>. Acesso em: 05 ago.2025.

BRANDÃO, I. C. (2025). **Crimes Cibernéticos e Engenharia Social**: A Evolução Tecnológica e seus Reflexos no Direito. [s.l.]: *Even3* Publicações, 29 mai. 2025, 23 p. Disponível em: <http://doi.org/10.29327/7565885>. Acesso em: 03 jun. 2025.

BRASIL (2018). **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais – LGPD. [*online*]. Brasília: Pres. República, [n.p.]. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 03 jun. 2025.

CERTBR (2021) – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil . **Cartilha de Segurança para Internet**. 13. ed. São Paulo: NIC.br, 126 p. Disponível em: <https://cartilha.cert.br>. Acesso em: 02 jun. 2025.

COHEN, F. (1987). **Computer Viruses**: Theory and Experiments. Computers & Security, v. 6, n. 1, p. 22–35.

COLE, E.; KRUTZ, R.L.; & CONLEY, J. (2005). ***Network Security Bible***. Idioma ingles. *New Jersey, EUA: John Wiley & Sons,* 694 p. ISBN: 978-0764573972.

DASWANI, N; & ELBAYADI, M. (*2021*). ***The Seven Habits of Highly Effective Security.*** Idioma Ingles. In: Grandes Violações. ISBN:978-1-4842-6655-7, *California: Apress, Berkeley, pp.195-232.* Disponível em: <https://doi.org/10.1007/978-1-4842-6655-7_9>. Acesso em: 02 jun. 2025.

DENNING, D. E. (1990). ***Information warfare and security***. Idioma Ingles. *Boston: Addison-Wesley*, 544 p.

PRIBERAM (2008-2025). **Dicionário Priberam da Língua Portuguesa** (em linha). [*online*]. [s.l.]: Priberam, [n.p.]. Disponível em: <https://dicionario.priberam.org/auto-excluir>. Acesso em: 02 jun. 2025.

EC-COUNCIL (2023). ***Certified Ethical Hacker (CEH ^{AI})***. *Train & Certify.* Idioma Ingles. Canadá: *EC-Council.* [n.p.]. Disponível em: <https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/>. Acesso em: 02 jun. 2025.

ENISA (2021). *European Union Agency for Cybersecurity.* ***Threat Landscape 2021 – Risks and Trend***s. Idioma Ingles. *Heraklion,* Grécia: ENISA, 113 p. Disponível em: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>. Acesso em: 02 jun. 2025.

ESET (2025). **O que é um *Trojan?* Como funciona e como se proteger**. *[online*]. [s.l.]: ESET. Disponível em: <https://www.eset.com/br/blog/cultura/o-que-e-um-trojan-como-funciona-e-como-se-proteger/>. Acesso em: 30 maio 2025.

FORTINET (2022). **O que é vírus de computador?** [*online*] *Blog*. [s.l.]: *Fortinet Inc*., [n.p.]. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/computer-virus#:~:text=Um%20v%C3%ADrus%20de%20computador%20%C3%A9,aos%20dados%20e%20ao%20software.>. Acesso em: 01 jun. 2025.

FORTINET (2025). **O que é um *Rootkit*? Como defendê-los e detê-los?** [*online*]. [s.l.]: *Fortinet*, [n.p.]. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/rootkit>. Acesso em: 01 jun. 2025.

HARARI, Y. N. (2018). **21 Lições para o Século 21**. Ed. Padrão, ISBN:978-8535930917. São Paulo: Companhia das Letras, 432 p.

IBGE (2022). **Pesquisa Nacional por Amostra de Domicílios Contínua - Tecnologia da Informação e Comunicação**. *[online]* .Rio de Janeiro: IBGE, [n.p.]. Disponível em: <https://www.ibge.gov.br/>. Acesso em: 04 jun. 2025.

IBM (2025). **A história do malware**: uma introdução à evolução das ameaças cibernéticas. [*online*]. Por Josh Schneider. [s.l.]: IBM, [n.p.]. Disponivel em: <https://www.ibm.com/br-pt/think/topics/malware-history>. Acesso em: 30 mai.2025.

IBM (2024). **O que é *ransomware?*** [*online*]. Idioma Ingles. [s.l.]: IBM. Disponível em: <https://www.ibm.com/br-pt/think/topics/ransomware>. Acesso em: 29 maio 2025.

KASPERSKY (2020a). **O que são vírus de computador?** [*online*]. Moscou: *Kaspersky Lab*. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/computer-viruses>. Acesso em: 01 jun. 2025.

KASPERSKY (2020b). ***Kaspersky Security Bulletin 2020. Statistics***. [*online*]. Idioma ingles. *Moscou: Kaspersky Lab*, [n.p.]. Disponível em: <https://securelist.com/kaspersky-security-bulletin-2020-statistics/99804/>. Acesso em: 30 mai. 2025.

KASPERSKY (2025a). ***Android Mobile Security Threats***. [*online*]. Idioma ingles. *Moscou: Kaspersky Lab*, [n.p.]. Disponível em: <https://www.kaspersky.com/resource-center/threats/mobile-malware>. Acesso em: 04 jun. 2025.

KASPERSKY (2025b). ***O que é jailbreak – definição e explicação***. [*online*]. *Moscou: Kaspersky Lab*, [n.p.]. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-jailbreaking>. Acesso em: 04 jun. 2025.

KIM, D.; & SOLOMAN, M. G. (2016). ***Fundamentals of Information Systems Security****: Print Bundle*. Idioma ingles. ISBN:9781284128239 3 ed, Jones & Bartlett Learning, 548 p. <https://books.google.com.br/books?id=kvBCDQAAQBAJ&redir_esc=y>. Acesso em: 04 jun. 2025.

LINKNACIONAL (2022). **Vírus de computador: o que são, como surgiram e como se proteger?** [*online*] *Blog*, Redação de Angélica Campos. Ribeirão Preto: Link Nacional, [n.p.]. Disponível em:

<https://www.linknacional.com.br/blog/virus-de-computador/?srsltid=AfmBOor8Tk9fgh5BeJasLXYkFECzTQbRKRRAjc2c1J82aOh2tNjxIn6Y>. Acesso em: 03 jun. 2025.

LUDWIG, M. (1998). ***The Giant Black Book of Computer Viruses.*** [*online*] *Pdf.* Idioma ingles. ed. 2, *Show Low, Arizona: American Eagle Publication*, 474 p. Disponível em: <https://ia802207.us.archive.org/30/items/TheGiantBlackBookOfComputerViruses2ndEd./The%20Giant%20Black%20Book%20of%20Computer%20Viruses%20%282nd%20ed.%29.pdf>. Acesso em: 03 jun. 2025.

MATTHEWS, T. (2022). ***Creeper*:** O primeiro vírus de computador do mundo. [s.l.]: *Exabeam*, [n.p.]. Disponível em: <https://www.exabeam.com/blog/infosec-trends/creeper-the-worlds-first-computer-virus/>. Acesso em: 02 jun. 2025.

MATHIAS, V. (2024). **A história da criação do primeiro vírus de computador do mundo começa com um adolescente de 15 anos e desenvolvimento de jogos.** [*online*]. [s.l.]: IGNBrasil Pub. 20 abr. 2024, [n.p.]. Disponível em: <https://content.time.com/time/magazine/article/0,9171,988152,00.html>. Acesso em: 02 jun. 2025.

MAYUMI, G; & RISA, T. (2024). **Segurança da Informação:** O primeiro vírus e o desenvolvimento da área. São Paulo: E Grupo PET-Sistemas de Informação - EACH/USP, [n.p.].

MITNICK, K. D.; & SIMON, W. L. (2002) ***The Art of Deception****: Controlling the Human Element of Security*. Idioma ingles. ISBN: 978-0764542800. 1 st, *Indianapolis: Wiley*, 368 p.

MITNICK, K.; SIMON, W. L. (1963/2003). **A arte de enganar**: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Tradução de Kátia Aparecida Roque. [*PDF*]. 1. ed., São Paulo: *Pearson Education* do Brasil Ltda, (1963) 2003, 587 p. Disponível em: https://www.ouka.com.br/carol/e-book/hacker/A%20Arte%20De%20Enganar%20-%20Kevin%20D.%20Mitnick.pdf. Acesso em: 22 jun. 2025.

NORTON (2021). ***How computer viruses spread***. [*online*]. Idioma ingles. *Mountain View: NortonLifeLock,* [n.p.]. Disponível em: <https://us.norton.com/blog/malware/how-computer-viruses-spread>. Acesso em: 03 jun. 2025.

OLHAR DIGITAL (2025). **Quais os melhores antivírus para PCs? Descubra como deixar seu computador protegido [2025]**.[*online*]. São Paulo: Olhar Digital, 2025, [n.p.]. Disponível em: <https://olhardigital.com.br/2025/01/22/seguranca/quais-os-melhores-antivirus-para-pcs-descubra-como-deixar-seu-computador-protegido-2025/>. Acesso em: 04 jun. 2025.

OKPA, J. T. *et al.* (2022). ***Cyberspace, Black-Hat Hacking and Economic Sustainability of Corporate Organizations in Cross-River State, Nigeria***. [*online*] *Pdf*. Idioma ingles. *12*(3), *California, USA*: *SAGE Open Original work published* 2022, 13 p. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/21582440221122739. Acesso em: 02 jun. 2025.

PALATTY, N. J. (2025), ***30+ Malware Statistics You Need to Know In 2025***. [*online*] *Blog*. Idioma ingles. [s.l.]: *Whatsnew.Getastra,* [n.p.]. Disponível em: <https://www.getastra.com/blog/security-audit/malware-statistics/>. Acesso em: 30 mai. 2025.

PALOALTO (2025). **O que é um ataque *denial-of-service* (rejeição de serviço - DOS)?** [*online*] Idioma ingles. *Cyberpedia*, [s.l.]: *Paloalto Networks,* [n.p.]. Disponível em: <https://www.paloaltonetworks.com.br/cyberpedia/what-is-a-denial-of-service-attack-dos>. Acesso em: 04 jun. 2025.

RUSSELL, S.; & NORVIG, P. (2016). ***Artificial Intelligence****: A Modern Approach.* [*online*] *Pd*f. Idioma ingles. ISBN: ISBN 0-13-103805-2, 3rd, *New Jersey: Prentice-Hall, Inc. A Simon & Schuster Company,* 946 p. Disponível em: <https://www.academia.edu/download/82860922/artificial_intelligence_modern_approach.9780131038059.25368.pdf>. Acesso em: 30 mai. 2025.

SCHNEIER, B. (1996). ***Applied Cryptography Protocols, Algorithms, and Source Code in C***. Idioma ingles. ISBN 978-1-119-09672-6. *20th Anniversary Hardcover*: ISBN:978-1-119-09672-6. *John Wiley & Sons*, 784 Pages.

SCHNEIER, B. (2015). ***Secrets and Lies:*** *Digital Security in a Networked World*. [*online*] *Libary,* ISBN:9781119183631. Idioma ingles. DOI:10.1002/9781119183631. [s.l.]: *John Wiley & Sons, Inc.,* 414 p. Disponível em: <https://doi.org/10.1002/9781119183631.fmatter>. Acesso em: 29 mai. 2025.

SILVA, I. **Romantização dos hackers**: por que precisamos parar de glamourizar o crime cibernético. [*online*]. [s.l.]: *TI* Inside, 28 out. 2025, [n,p.]. Disponível em: <https://tiinside.com.br/28/10/2025/romantizacao-dos-hackers-por-que-precisamos-parar-de-glamourizar-o-crime-cibernetico>. . Acesso em: 30 out. 2025.

SKOUDIS, E.; & ZELTSER, L. (2003). ***Malware****: Fighting Malicious Code.* Idioma ingles. ISBN:0131014056, 9780131014053. *New Jersey, United States: Prentice Hall PTR* 647 p.

SOUZA, R. de (2020). **Em 2020, pelo menos 360 mil vírus para computador foram criados por dia**. [*online*]. [s.l.]: Canaltech, [n.p.]. Disponível em: <https://canaltech.com.br/seguranca/em-2020-pelo-menos-360-mil-virus-para-computador-foram-criados-por-dia-176642/>. Acesso em: 01 jun. 2025.

SPAFFORD, E. H. (1994). *Computer viruses as artificial life. In:* ***Artificial Life III: Proceedings of the Workshop on Artificial Life***. *Santa Fe Institute Studies in the Sciences of Complexity*. *Redwood City: Addison-Wesley*, p. 741–765.

STALLINGS, W. (2019). ***Computer Security:*** *principles and practice*. Idioma ingles. 4. ed. *Boston: Pearson,* 720 p.

STAMP, M. (2005). ***Information Security****: Principles and Practice*. Idioma ingles. ISBN: 978-0-471-74418-4, *October 2005*. [s.l.]: *John Wiley & Sons, Inc.*, 368 p.

SYMANTEC (2020). ***Types of computer viruses****.* [*online*]. *Mountain View: Symantec Corporation.* Idioma ingles. Disponível em: <https://www.symantec.com/blogs>. Acesso em: 30 mai. 2025.

SYMANTEC (2021). ***Internet Security Threat Report***. [*online*] *Pdf*. Idioma ingles. *Mountain View: Symantec Corporation,* 98 p. Disponível em: <https://www.symantec.com/security-center>. Acesso em: 01 jun. 2025.

TANENBAUM, A. S.; & WETHERALL, D. J. (2011) **Redes de computadores**. 5ª ed. São Paulo: *Pearson*.

TANENBAUM, A. S. (2015). ***Modern operating systems***. Idioma ingles. 4ª ed. *Upper Saddle River: Prentice Hall*, 1136 p.

TECHTUDO (2018). **O que é um *worm?* Entenda o *malware* que se multiplica sozinho**. Rio de Janeiro: Globo.com, [n.p.]. Disponível em: <https://www.techtudo.com.br/noticias/2018/11/o-que-e-um-worm-entenda-o-malware-que-se-multiplica-sozinho.ghtml >. Acesso em: 01 jun. 2025.

THOMAS, B (2023). ***The First Computer Virus of Bob Thomas Explained****: Everything You Need to Know*. [*online*]. Idioma ingles. [s.l.]: *History-Computer*, [n.p.]. Disponível em: <https://history-computer.com/the-first-computer-virus-of-bob-thomas/>. Acesso em: 30 mai. 2025.

UHD (2025a). ***Computer Virus Fact Sheet.*** [*online*] Idioma ingles. *Houston: University of Houston-Downtown*, [n.p.]. Disponível em: <https://www.uhd.edu/computing/uss/computer-virus-fact-sheet.aspx>. Acesso em: 29 mai. 2025.

UHD (2025b). ***How to Remove Spyware from Your Computer.*** [*online*] Idioma ingles. *Houston: University of Houston-Downtown*, [n.p.]. Disponível em: <https://www.uhd.edu/>. Acesso em: 03 jun. 2025.

UOL (2021). **Como descobrir um vírus no seu celular? Siga estes 7 passos... Veja mais em**. Rio: UOL *Tilt*, [n.p.]. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/06/26/como-descobrir-um-virus-no-seu-celular-siga-estes-7-passos.htm?cmpid=copiaecola>. Acesso em: 04 jun. 2025.

UOL (2024). **IBGE revela que Brasil tem 163,8 milhões de pessoas com aparelho de telefone celular**. [*online*], Rio: Estadão Universo *Online,* [n.p.]. Disponível em:<https://economia.uol.com.br/noticias/estadao-conteudo/2024/08/16/ibge-revela-que-brasil-tem-1638-milhoes-de-pessoas-com-aparelho-de-telefone-celular.htm>. Acesso em: 03 jun. 2025.

USCSI (2024). ***Understanding the difference between Black, White, and Gray-Hat Hackers***. [*online*] *Blog,* Idioma ingles. *United States Cybersecurity Institute*. *Arlington, Virgínia: USCSI, 29, Apr,* 2024, [n.p.]. Disponível em: <https://www.uscsinstitute.org/cybersecurity-insights/blog/understanding-the-difference-between-black-white-and-gray-hat-hackers>. Acesso em: 03 jun. 2025.

WACK, J.; & TRACY M. (2003). NIST SP 800-42: ***Guideline on Network Security Testing***. [online]. *Computer Security Resource Center* [s.l.]: NIST/CSRC, pub. Oct. 2003, [n.p.]. Disponível em: <https://csrc.nist.gov/pubs/sp/800/115/final>. Acesso em 25 jun. 2025.

WIKI (2023). **Falha (tecnologia).** Enciclopédia [*online*]. [s.l.]: *Wikipedia,* 15 dez. 2023, [n.p.]. Disponível em: <https://pt.wikipedia.org/wiki/Falha_(tecnologia)Acesso em: 01 jun.2025.

WIKI (2024a). ***BBN Time-Sharing System.*** Enciclopédia [*online*]. [s.l.]: *Wikipedia,* 18 jun. 2024, [n.p.]. Disponível em: <https://en.wikipedia.org/wiki/BBN_Time-Sharing_System> Acesso em: 01 jun.2025.

WIKI (2024b). ***Brain* (vírus de computador).** Enciclopédia [*online*]. [s.l.]: *Wikipedia,* 20 Nov 2024, [n.p.]. Disponível em: <https://pt.wikipedia.org/wiki/Brain_(vírus_de_computador)>. Acesso em: 01 jun.2025.

WIKI (2025a). ***Certified ethical hacker***. *Enciclopédia*. [*online*]. [s.l.]: *Wikipedia, 20 May* 2025, [n.p.]. Disponível em: <https://en.wikipedia.org/wiki/Certified_ethical_hacker>. Acesso em: 29 mai. 2025.

WIKI (2025b). ***White hat (computer security)***. Enciclopédia [*online*]. [s.l.]: *Wikipedia, 26 May* 2025, [n.p.]. Disponível em: <https://en.wikipedia.org/wiki/White_hat_(computer_security)>. Acesso em: 30 mai.2025.

ZETTER, K. (2014). ***Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon***. Idioma ingles. ISBN:9780770436179, *Midtown Manhattan: Crown Publishers,* 433 p.