

Detecção de malware em instituições de ensino superior: uma revisão das ameaças de phishing, ransomware e DDoS

Malware detection in higher education institutions: a review of phishing, ransomware, and DDoS threats

Detección de malware en instituciones de educación superior: una revisión de las amenazas de phishing, ransomware y DDoS

Carlos Eduardo da Cunha Silva

Mestrando em Engenharia Elétrica aplicada à Segurança Cibernética
Instituição: Universidade de Brasília
Endereço: Brasília – Distrito Federal, Brasil
E-mail: carloscarioka@unb.br

Edinei Coelho Ferreira

Mestrando em Computação Aplicada à Ciência de Dados
Instituição: Universidade de Brasília
Endereço: Curitiba – Paraná, Brasil
E-mail: edineipmbok@gmail.com

Luis Marcos Martins do Nascimento

Mestrando em Engenharia Elétrica aplicada à Segurança Cibernética
Instituição: Universidade de Brasília
Endereço: Brasília – Distrito Federal, Brasil
E-mail: luismarcos@unb.br

João Goulart Batista Reis

Mestrando em Engenharia Elétrica aplicada à Segurança Cibernética
Instituição: Universidade de Brasília
Endereço: Brasília – Distrito Federal, Brasil
E-mail: jango@unb.br

Daniel Chaves Café

Doutor em Ciências e Tecnologia em Tecnologia da Informação, Telecomunicações e Sistemas
Instituição: École Supérieure d'Électricité
Endereço: Gif-sur-Yvette – França
E-mail: dcafe@unb.br

RESUMO

Nos últimos anos, as instituições de ensino superior têm sido alvo cada vez mais frequente de ataques cibernéticos que comprometem a confidencialidade, a integridade e a disponibilidade de dados acadêmicos e administrativos. Este estudo apresenta uma revisão sistemática das práticas e técnicas de detecção de *malware* em ambientes de ensino superior, com foco nas ameaças de *phishing*, *ransomware* e ataques de negação de serviço distribuído (DDoS). A revisão evidencia

que as universidades continuam sendo alvos recorrentes de ataques devido à abertura de seus sistemas, à diversidade de dispositivos conectados e à circulação constante de informações sensíveis relacionadas a estudantes, servidores e pesquisas científicas. As estratégias de detecção discutidas nos estudos analisados incluem mecanismos comportamentais, modelos de aprendizado de máquina, análise de padrões de tráfego de rede, inspeção de anomalias e técnicas híbridas que integram métodos estáticos e dinâmicos de identificação de ameaças. Para consolidar os achados e integrar diferentes resultados metodológicos, utilizou-se a Teoria do Enfoque Meta-Analítico Consolidado (TEMAC), ferramenta aplicada na revisão de literatura que teve como base as seguintes palavras-chave: *phishing*, *ransomware*, ataques DDoS, *malware*, instituições de ensino superior e detecção. Para chegar aos resultados foram utilizadas bases de dados da plataforma de pesquisa Web of Science e IEEE Xplore, entre 2021-2025. Após a extração dos dados do WoS (400) e IEEE (355) os dados foram concatenados e após o processamento dos 755 artigos coletados observou-se a duplicidade de 49 que foram removidos, restando a diferença de 706 arquivos úteis para a pesquisa. O trabalho referenciou cinco artigos mais citados e os outros sete que contribuíram para soluções de possíveis problemas relacionados aos ataques cibernéticos. O trabalho teve o auxílio de 31 referências essenciais para fluidez do estudo.

Palavras-chave: phishing, ransomware, ataques DDoS, malware, instituições de ensino superior, detecção.

ABSTRACT

In recent years, higher education institutions have been increasingly targeted by cyberattacks that compromise the confidentiality, integrity, and availability of academic and administrative data. This study presents a systematic review of malware detection practices and techniques in higher education environments, focusing on phishing threats, ransomware, and distributed denial-of-service (DDoS) attacks. The review shows that universities continue to be recurring targets of attacks due to the openness of their systems, the diversity of connected devices, and the constant circulation of sensitive information related to students, servers, and scientific research. The detection strategies discussed in the studies analyzed include behavioral mechanisms, machine learning models, network traffic pattern analysis, anomaly inspection, and hybrid techniques that integrate static and dynamic threat identification methods. To consolidate the findings and integrate different methodological results, the Consolidated Meta-Analytic Approach Theory (TEMAC) was used, a tool applied in the literature review based on the following keywords: phishing, ransomware, DDoS attacks, malware, higher education institutions, and detection. To obtain the results, databases from the Web of Science and IEEE Xplore research platforms were used between 2021 and 2025. After extracting the data from WoS (400) and IEEE (355), the data were concatenated, and after processing the 755 articles collected, 49 duplicates were removed, leaving 706 files useful for the research. The study referenced five most cited articles and seven others that contributed to solutions for possible problems related to cyber attacks. The study was aided by 31 essential references for the fluidity of the study.

Keywords: phishing, ransomware, DDoS attacks, malware, higher education institutions, detection.

RESUMEN

En los últimos años, las instituciones de educación superior han sido objeto cada vez más frecuente de ciberataques que comprometen la confidencialidad, la integridad y la disponibilidad de los datos académicos y administrativos. Este estudio presenta una revisión sistemática de las prácticas y técnicas de detección de malware en entornos universitarios, centrándose en las amenazas de phishing, ransomware y ataques de denegación de servicio distribuido (DDoS). La revisión pone de manifiesto que las universidades siguen siendo objetivos recurrentes de los ataques debido a la apertura de sus sistemas, la diversidad de dispositivos conectados y la circulación constante de información sensible relacionada con los estudiantes, los servidores y las investigaciones científicas. Las estrategias de detección discutidas en los estudios analizados incluyen mecanismos de comportamiento, modelos de aprendizaje automático, análisis de patrones de tráfico de red, inspección de anomalías y técnicas híbridas que integran métodos estáticos y dinámicos de identificación de amenazas. Para consolidar los hallazgos e integrar los diferentes resultados metodológicos, se utilizó la Teoría del Enfoque Meta-Analítico Consolidado (TEMAC), una herramienta aplicada en la revisión de la literatura que se basó en las siguientes palabras clave: phishing, ransomware, ataques DDoS, malware, instituciones de educación superior y detección. Para obtener los resultados se utilizaron bases de datos de la plataforma de investigación Web of Science e IEEE Xplore, entre 2021 y 2025. Tras extraer los datos de WoS (400) e IEEE (355), se concatenaron y, tras procesar los 755 artículos recopilados, se observó la duplicación de 49, que se eliminaron, quedando una diferencia de 706 archivos útiles para la investigación. El trabajo hizo referencia a los cinco artículos más citados y a los otros siete que contribuyeron a la solución de posibles problemas relacionados con los ciberataques. El trabajo contó con la ayuda de 31 referencias esenciales para la fluidez del estudio.

Palabras clave: phishing, ransomware, ataques DDoS, malware, instituciones de educación superior, detección.

1 INTRODUÇÃO

As instituições de ensino superior estão enfrentando desafios crescentes e raros em relação à segurança cibernética, tornando-se alvos chave de ataques devido à grande quantidade de metadados armazenados em seus bancos de dados institucionais. Esses ambientes acadêmicos produzem materiais de alto valor, como dissertações, artigos científicos, pesquisas de doutorado e pós-doutorado, que despertam grande interesse de agentes mal-intencionados.

Os ataques aos sistemas das instituições de ensino superior são os que alimentam o apetite dos criminosos virtuais, principalmente na produção de conteúdo e didáticas virtuais deles. O Moodle é um sistema de Gestão de Aprendizagem, ou seja, uma plataforma *on line* que proporciona em seu ambiente aulas virtuais e interação dos discente aos docentes através de

tarefas e avaliações. Além disso, armazena dados sensíveis como conteúdo, identificações de alunos, professores e credenciais corporativas. Como é um sistema que armazena metadados sensíveis e de cunho científico e pessoal a segurança automatizada dos dados e de suma relevância (Nascimento *et al*, 2025).

Segundo Nascimento (2025), a automatização de um sistema robusto como do *Moodle* é necessário para que não ocorra incidências de falhas humanas, retrabalho e vulnerabilidades a scripts maliciosos. Para isso, foi desenvolvido o PRP01 (*Palton's Robot in Python*) foi programado para integrar o *Moodle* com os sistemas institucionais SIGAA e SINGER através da *web scraping* e autenticação segura.

Em virtude do amplo volume de metadados gerados pelas instituições de ensino, o interesse dos invasores tem se intensificado, já que essas informações incluem pesquisas valiosas e dados confidenciais de valores inestimáveis. Segundo Ulver e Wanger (2021), as instituições geram um quantitativo substancial de metadados dados sensíveis e importantes, o que fomenta e deixa atrativo aos cibercriminosos (atacantes), principalmente a extensão do mercado ilegal que financia com valores expressivos para obter os dados pessoais e resultados de pesquisas, tornando o fluxo de ataques ainda mais frequente.

Não basta reduzir de forma expressiva os ataques e práticas de cyberespionagem neste contexto tecnológico, mas também deve-se compreender os vetores de ataque e fatores culturais que precisam ser identificados e debatidos. Para reduzir essas ameaças de forma eficaz, é essencial adotar medidas preventivas voltadas ao monitoramento contínuo das tentativas de intrusão, bem como à identificação dos principais tipos de vulnerabilidades e riscos que afetam esses ambientes acadêmicos (Ulver e Wanger, 2021).

Além disso, estudos recentes investigaram os principais tipos de ameaças digitais enfrentadas pelas universidades, revelando vulnerabilidades críticas em seus sistemas. Entre as ameaças mais recorrentes destacam-se o *phishing* e a engenharia social reversa, considerados vetores predominantes de invasões externas. O *ransomware* e ataques envolvendo SQL também se mostram particularmente preocupantes, pois a primeira causa paralisações operacionais e danos aos sistemas, enquanto o segundo injeta códigos maliciosos para obter acesso ilegal a dados confidenciais (Pillay e Sharma, 2023).

De acordo com Pillay e Sharma (2023), ataques envolvendo *phishing*, *ransomware* e SQL têm preocupado especialistas, que observam um crescimento significativo dessas ocorrências em universidades públicas e privadas, impulsionado pelo valor estratégico do conteúdo armazenado.

Pillay e Sharma (2023, p. 2) acrescentam um fator importante que,

[...]visar reitores de universidades ou membros acadêmicos específicos é uma tática alternativa. Essas pessoas podem ter acesso a determinados conjuntos de dados que interessam aos hackers, ou podem simplesmente ser pessoas abastadas. Para escolher a melhor estratégia para ganhar confiança da pessoa-alvo, o hacker examinará o seu comportamento. Essa tática também é conhecida como “*whaling*” ou “*spear phishing*”.

Com isso, torna-se evidente a necessidade de melhoria contínua principalmente no que tange as políticas e práticas de segurança cibernética no ambiente de ensino superior. A implementação de medidas robustas, como atualizações regulares de software, protocolos avançados de autenticação e ações permanentes de conscientização dos usuários, é essencial para mitigar riscos e assegurar a continuidade das atividades educacionais e administrativas.

O artigo foi organizado da seguinte forma: resumo após esta a seção 1 introdução, seguido da seção 2 que apresenta o referencial teórico, no qual são discutidos alguns ataques cibernéticos relevantes para universidades, tais como *phishing*, *ransomware*, *DDoS* e *malware*; a seção 3 detalha a metodologia utilizada e, em seu subitem, descreve a revisão sistemática realizada com base na Teoria do Enfoque Meta-Analítico Consolidado (TEMAC); a seção 4 apresentação dos resultados e análises; e, por fim, a seção 5 traz a conclusão do estudo.

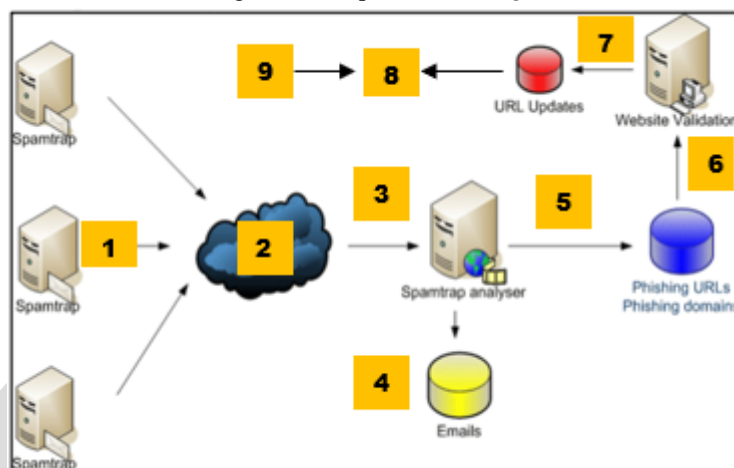
2 REFERENCIAL TEÓRICO

2.1 PHISHING

O *Phishing* é uma técnica de engenharia social reversa que é utilizada para ludibriar a vítima e a induzi-la a expor dados privados, e após a execução de ações que comprometam sua segurança digital. A vítima ao clicar em link duvidoso este se manifesta instalando programas hospedeiros mal-intencionados (*malware*) em seus dispositivos. De acordo com Neves (2022), trata-se de um método simples, porém altamente eficiente e amplamente utilizado em larga escala. Durante a pandemia de COVID-19, esse tipo de golpe se intensificou, pois, os atacantes

exploravam a vulnerabilidade emocional e o estado de fragilidade das pessoas para aumentar a eficácia das fraudes. Abaixo na Figura 1 segue um exemplo de um sistema de proteção contra ataques de *phishing*.

Figura 1. Ataque de *Phishing*



Fonte: Pillay e Sharma (2023) Adaptado.

A abaixo segue o fluxo lógico traduzido do sistema acima (Pillay e Sharma, 2023):

- 1º. **Central de Spam** – representam os inúmeros pontos de origem das mensagens maliciosas (E-mails fraudulentos), normalmente distribuídos em larga escala pelos atacantes;
- 2º. **Rede de Internet (Nuvem)** – representa os diversos pontos de origem e o percurso das mensagens suspeitas até o servidor de análise, constituindo o canal de comunicação pelo qual os e-mails trafegam antes de serem inspecionados;
- 3º. **Servidor Analisador de Spamtraps** – atua como um núcleo do sistema, recebendo os e-mails coletados e realizando:
 - a) Inspeção do conteúdo da mensagem;
 - b) Análise de cabeçalhos (*headers*);
 - c) Identificação de padrões típicos de *phishing* (*links* suspeitos, linguagem fraudulenta e domínios falsos).
- 4º. **Base de Dados de E-mails** – Armazena as mensagens analisadas, permitindo:
 - a) Auditoria e rastreabilidade;
 - b) Treinamento de mecanismos de detecção (regras de inteligência artificial);
 - c) Correlação com incidentes anteriores.

5º. Extração e classificação de URL's – Durante a análise, os links contidos nos e-mails os dados são extraídos para verificação específica, pois normalmente o link direciona para uma página falsa.

6º. Validação de Websites (Websites Validation) – As URL's são acessadas em ambiente controlado para verificar:

- a) Autenticidade do Site;
- b) Presença de formulários Fraudulentos;
- c) Tentativa de coleta indevida de credencias.

7º. Atualização de URL's (URL's Updates) – URL's confirmadas como maliciosa são registradas continuamente em listas de bloqueio (*blacklist*).

8º. Base de Dados de URL's de Phishing e Domínios Maliciosos – Consolida os endereços identificados como *phishing*, permitindo:

- a) Bloqueio preventivo de acessos futuros;
- b) Compartilhamento de informações com outros sistemas de segurança;
- c) Redução do risco de reincidência do ataque.

9º. Resultado Final do Sistema – O conjunto de processos permite detectar, classificar, registrar e bloquear ataques de phishing de forma proativa proporcionada proteção ao usuário de roubo de credencias, fraudes financeiras e comprometimento do sistema.

Entretanto nessas situações, o invasor realiza um estudo prévio detalhado sobre o comportamento da vítima. Ele analisa padrões de comunicação, hábitos profissionais, redes de contato e informações públicas divulgadas em sites institucionais ou redes sociais. (Pillay e Sharma, 2023).

Após a coleta dos metadados, os criminosos cibernéticos estruturam abordagens altamente personalizadas, capazes de proporcionar e transmitir a vítima credibilidade e confiança, aumentando significativamente o percentual de intrusão aqueles dados almejados (Ulven e Wanger, 2021).

Em vez de enviar mensagens genéricas para um grande número de pessoas, o criminoso concentra seus esforços em poucos alvos estratégicos, desenvolvendo mensagens sofisticadas e bem elaboradas. Essa personalização torna a ameaça particularmente perigosa, pois dificulta a detecção por filtros de segurança e aumenta a probabilidade de que a vítima interaja com o conteúdo malicioso (Neves, 2022).

2.2 RANSOMWARE

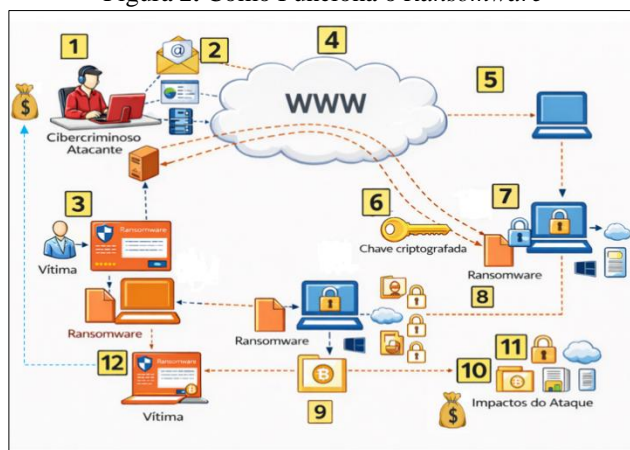
Outro problema de *malware* considerado mais grave que afeta escolas, institutos e universidades atualmente é o avanço dos ataques de *ransomware*. Esse tipo de *software* malicioso invade os sistemas da vítima, localiza arquivos sensíveis — como dados acadêmicos, administrativos e pesquisas científicas — e os bloqueia por meio de criptografia. Somente após esse sequestro digital o invasor exige um pagamento para devolver o acesso aos dados. Instituições de ensino superior, por armazenarem informações de alto valor e conduzirem pesquisas estratégicas, são alvos recorrentes desse tipo de ataque (Cheng e Wang, 2022).

De acordo com Cheng e Wang (2022), as consequências de um ataque de ransomware podem ser devastadoras para qualquer universidade. Além do pedido de resgate, que costuma envolver valores extremamente elevados, há impactos diretos sobre a operação institucional. Sistemas inteiros podem ficar inacessíveis, prejudicando atividades acadêmicas, administrativas, científicas e financeiras.

A perda de dados, a paralisação prolongada de serviços e a interrupção do calendário acadêmico podem gerar danos duradouros, inclusive afetando o planejamento anual e a execução de pesquisas financiadas por agências públicas e privadas (Lachi, 2021).

Outro ponto crítico é o dano à reputação da instituição. Quando informações sensíveis são sequestradas, corrompidas ou divulgadas por criminosos, a confiança de estudantes, servidores, pesquisadores e parceiros externos pode ser profundamente abalada. Na Figura 2 temos um exemplo de como funciona o *Ransomware* (Lallie, H. Singh. *et al*, 2021).

Figura 2. Como Funciona o *Ransomware*



Fonte: Pillay e Sharma (2023) Adaptado.

Para compreender melhor esse cenário, modelos explicativos como “Como Funciona o *Ransomware*” detalham o ciclo do ataque: desde a infecção inicial (geralmente por *phishing* ou vulnerabilidades não corrigidas), passando pela fase de criptografia silenciosa dos dados, até a exibição da mensagem de resgate. Esse entendimento é fundamental para reforçar políticas de prevenção, resposta rápida e resiliência cibernética no ambiente acadêmico (Pillay e Sharma, 2023). A abaixo segue o fluxo lógico traduzido do sistema acima (Pillay e Sharma, 2023):

1º. Atacante (*Hacker* / Grupo Criminoso) – É conceituado como agente malicioso que desenvolve ou utiliza o *malware* e define qual vetor de ataque será lançado (e-mail, site fraudulento etc.);

2º. Vetor de Infecção Inicial – O ataque geralmente começa por:

- a) E-mail de *phishing* com anexo ou link malicioso;
- b) *Download* de *software* infectado;
- c) Exploração de vulnerabilidades em sistemas ou serviços à internet;

3º. Infecção da Vítima Inicial – O usuário executa o arquivo ou acessa o link, permitindo que o *ransomware* seja instalado no computador ou servidor;

4º. Conexão com a Internet (WWW) – Após a infecção, o *malware* se comunica com servidores externos controlados pelo atacante, normalmente para:

- a) Enviar informações do sistema infectado;
- b) Obter instruções adicionais;
- c) Receber chaves ou parâmetros de criptografia.

5º. Geração/ Recebimento da Chave de Criptografia – O *malware ransomware* utiliza algoritmos criptográficos (simétricos ou assimétricos) para gerar ou receber a chave que será utilizada para lesar a vítima;

6º. Criptografia dos Arquivos – Os dados do sistema infectado (documentos, imagens, bancos de dados entre outros) são criptografados pelo atacante tornando-os inacessíveis ao usuário legítimo;

7º. Propagação na Rede Interna – Em ambientes corporativos, o *ransomware* pode espalhar para outros computadores com o objetivo de explorar:

- a) Credencias compartilhadas;
- b) Pastas de rede;
- c) Vulnerabilidades não mitigadas.

8°. Infecção de Outras Máquinas – Após alguns ataques efetivados e bem-sucedidos outros dispositivos passam a sofrer com o mesmo processo de criptografia, ampliando assim a proporção e os impactos dos ataques;

9°. Mensagem de Resgate – Após o sucesso com a criptografia ao sistema infectado o atacante lança uma mensagem a vítima informando que:

- a) Seus arquivos pessoais foram bloqueados e capturados;
- b) Os valores das informações sequestradas devem ser pagos por criptomoedas;
- c) As instruções para pagamento e contato com o atacante.

10°. Exigências de Pagamento – O Criminoso Cibernético condiciona a vítima a chave de descryptografia condicionado ao pagamento de um resgate, mas não garante a recuperação dos dados sequestrados.

11°. Impactos dos Ataques – A intrusão de um sistema pode proporcionar a vítima indisponibilidade das informações, prejuízos financeiros, risco a sua reputação a depender de qual conteúdo poderá ser divulgado e perda definitiva de seus dados.

12°. Conclusão do Ciclo – O ataque é considerado completo quando a vítima:

- a) Paga o resgate (com ou sem a recuperação dos dados), ou
- b) Restaura os sistemas a partir de backups e medidas de resposta a incidentes

2.3 DDOS

Os ataques distribuídos de negação de serviço (DDoS) são considerados como técnicas de ataques cibernéticos e não códigos maliciosos, ou seja, não é um *malware*. A ideia desta técnica de ataque proporcionado pelos cibercriminosos é injetar um quantitativo expressivo de tráfego na rede. O intuito desta expertise é consumir os recursos da rede atacada e proporcionar lentidão, perturbar os sistemas e serviços da universidade como e-mails, web sites além de congestionamento na rede (Ma Haque, Md. *et al*, 2023).

Segundo o Dolliver, D. *et al* (2021), os ataques de DDoS seguem duas metodologias de aplicação. Na primeira, o cibercriminoso modela uma rede de ataques distribuídas por meio de *zombies*, robôs ou *hots* de intrusão. Esses ciberataques proporcionam danos para aos usuários atacados por um DDoS vão além da simples interrupção de serviços.

De acordo Lachi e Anatolie, (2022) o campo de ensino superior tem sido alvo em relação as pesquisas realizadas e com isso proporcionam um apetite interessante aos ciberespíões. Relatam em seu artigo que ocorreu um aumento expressivo de 350% de intrusões por meio de ataques de DoS/DDoS, direcionados principalmente ao ensino à distância.

Em muitos casos a paralisação de sistemas críticos acarreta perdas financeiras, atrasos em projetos e danos à reputação institucional, especialmente quando afeta serviços que suportam atividades administrativas e científicas.

Além disso, ataques DDoS podem ser usados como cortina de fumaça para outras intrusões simultâneas, como roubo de dados ou instalação de *malware*, ampliando ainda mais o grau de risco para a universidade e seus usuários (Fan, C. *et al*, 2021).

Em suma, as ameaças cibernéticas têm sido identificadas nas instituições de ensino superior, destacando-se entre as mais recorrentes o *phishing*, as ameaças internas, os ataques distribuídos de negação de serviço (DDoS), as violações de dados e o *ransomware*. O autor menciona dois potenciais de intrusão um é o *hacker*, que proporcionam ataques externos e outra interna chamada de Zona Desmilitarizada (DMZ) que está dentro do Local Area Network (LAN) (Naagas, M. *et al*. 2018).

Por isso, a urgência em fortalecer a segurança digital nas universidades por meio de soluções mais avançadas, especialmente aquelas baseadas em inteligência artificial, capazes de detectar padrões anômalos, antecipar comportamentos suspeitos e mitigar ataques antes que causem danos significativos são de extrema relevância (Naagas, M. *et al*. 2018).

2.4 MALWARE

O abreviamento de software malicioso "*malware*" se refere-a programas projetados com o objetivo de adentrar de forma ilegal em um sistema computacional para subtrair, capturar, manipular ou danificar informações valiosas de cunho restrito e pessoal. Softwares maldosos podem ser distribuídos a rede a ser atacada por diferentes códigos de intrusão, como *worms*, *ddos*, e *ransomware* e vírus considerados simples, que aproveitam a vulnerabilidades para se propagar e atingir seus objetivos criminosos e ilícitos (Ferreira, L. *et al*.2023).

A disseminação dos códigos maliciosos pode ocorrer através de e-mails fraudulentos, sites maliciosos e duvidosos, mídias removíveis infectadas ou até mesmo por anexos de arquivos

aparentemente inofensivos que, ao serem executados (abertos), podem liberar diversos códigos nocivos e destrutivos ao sistema da vítima (Rajput, P. *et al.* (2021).

No entanto, o programa malicioso evoluiu de forma expressiva ao longo dos anos, se tornou um exemplo de sofisticação de modelagem dificultando o seu detectar. Modelos avançadíssimos, como ofuscação de código, polimorfismo e uso de inteligência artificial, permitem que esses *softwares* maliciosos se adaptem para ludibriar os antivírus tradicionais e sistemas de detecção baseados em assinaturas criptográficas. Com isso, as instituições e usuários comuns enfrentam ameaças crescentes, exigindo estratégias de segurança mais robustas e atualizadas (Ferreira, L. *et al.* 2023).

Em um contexto global, as intrusões realizadas pelos cibercriminosos através de programas maliciosos podem gerar impactos expressivos e as vezes sem reparação, como falhas e interrupção de serviços, vazamento de metadados sensíveis, prejuízos financeiros e danos à reputação. Instituições de nível superior, órgãos estatais e empresas privadas vem se tornam alvos frequentes devido ao grande quantitativo de dados armazenados e ao uso intensivo de redes compartilhadas, o que facilita a ação de agentes criminosos caso não exista políticas adequadas de proteção digital (Ma Haque, Md. *et al.* 2023).

Finalizando o item a prevenção aos programas maliciosos *malware* exige dos especialistas uma abordagem multidisciplinar que envolve tecnologia, processos e principalmente o comportamento humano. Técnicas básicas a serem utilizadas como autenticação forte, backups regulares, uso de ferramentas de análise comportamental, atualização constante de sistemas e capacitação dos usuários são fundamentais para reduzir riscos de ataques (Rajput, P. *et al.* 2021).

Com o avanço contínuo das ameaças cibernéticas, investir em segurança digital deixou de ser uma opção e passou a ser uma necessidade indispensável para qualquer ambiente conectado.

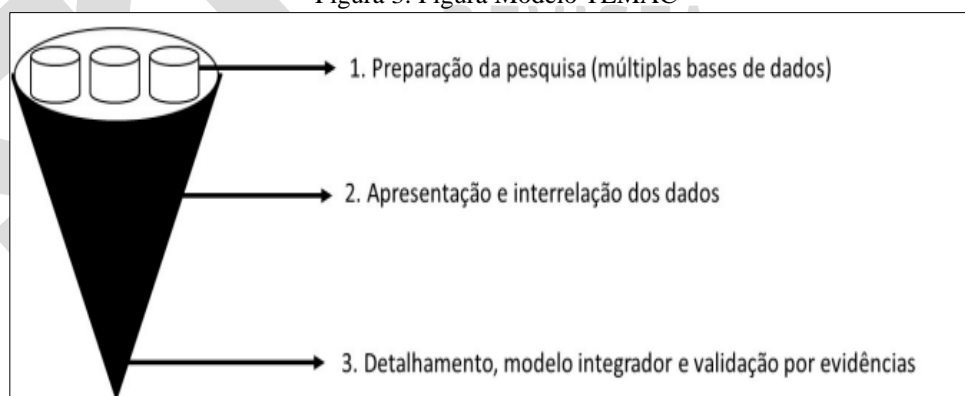
3 METODOLOGIA

A Teoria do Enfoque Meta-Analítico (TEMAC) é apresentada como uma metodologia bem estruturada para revisão bibliográfica, com a ideia de integrar e organizar grandes quantidades de metadados científicos (Ferreira, L. *et al.* 2023).

Entretanto a técnica utiliza métricas chamadas de bibliométricos, e com isso o TEMAC permite mapear o estado atual de um tema e identificar padrões significativos na produção acadêmica. É um modelo que pode ser aplicado em diversas áreas do conhecimento, sendo especialmente útil para pesquisadores que estão começando a explorar um assunto e precisam entender seu contexto teórico e metodológico (Mariano e Rocha, 2017).

O método se desdobra em três fases bem definidas. A fase de preparação é o planejamento de como será modelada a pesquisa denominada como inicial, onde se define o escopo, as fontes de informação e os critérios para a seleção dos estudos. Depois vem a organização e análise das informações, momento em que os dados coletados são apresentados, categorizados e comparados. Por último, o método avança para a fase de refinamento e validação, onde se constroem modelos integradores e se confirmam os achados com base nas evidências reunidas (Ferreira, L. *et al.* 2023). Figura 3 Modelo TEMAC.

Figura 3. Figura Modelo TEMAC



Fonte: Mariano e Rocha (2017)

Os potenciais principais do TEMAC são a sua capacidade de identificar tendências científicas ao longo do tempo. Ele permite observar os temas estão se tornando mais relevantes, os que estão perdendo força e quais disciplinas pouco exploradas ou necessitam de mais pesquisas. Esse panorama ajuda a definir lacunas, identificar oportunidades de investigação e traçar direções estratégicas para novos estudos (Ferreira, L. *et al.* 2023).

Primeiro, Planejamento da pesquisa: São selecionados os termos de pesquisa com base em palavras-chave relevantes do tema e das disciplinas relacionadas. Após essa decisão, é realizada uma pesquisa sistemática nas bases de dados selecionadas, de acordo com a estrutura pré-determinada (Mariano e Rocha, 2017).

A segunda tratará da apresentação e correlação de dados que se baseia na catalogação dos registros descobertos, o que inclui a determinação das publicações mais proeminentes, o surgimento cronológico das publicações, os documentos mais citados, bem como a análise do impacto das nações, ocorrências históricas, instituições acadêmicas, agências de financiamento e terminologia frequentemente utilizada (Mariano e Rocha, 2017).

Por fim, a terceira fase, aprofundamento, modelo de integração e confirmação por dados, apresenta análises detalhadas, tais como redes de colaboração e citações, conceitos centrais e caminhos de pesquisa. Essa fase facilita a comparação de resultados entre várias fontes e contribui para o desenvolvimento de um modelo integrativo que resume com precisão, tanto teórica quanto praticamente, as conclusões da investigação (Mariano e Rocha, 2017).

4 RESULTADOS E DISCUSSÕES

4.1 ETAPA I - PLANEJAMENTO DA PESQUISA

Neste primeiro momento do trabalho científico, será informado os métodos de buscas que foram utilizados. A base de dados utilizada para compor os resultados e discussões foram o *Web of Science* coleção principal (Clarivate) e *IEEE Xplore*, por proporcionarem uma base confiável e reconhecida internacionalmente elas foram escolhidas para compor os resultados. (Adriaanse e Rensleigh, 2013).

O trabalho de mineração simples dos dados bases tiveram o início entre os períodos de 07/10/2025 a 12/01/2026. As proposições lógicas conectivas utilizadas nas pesquisas avançadas nas bases de dados podem ser analisadas na Tabela 1. Após análise dos dados foram obtidos os seguintes resultados: 400 resultados da base de dados do *Web of Science* e 355 resultados da base de dados da *IEEE Xplore*.

Para chegar nos resultados do tema proposto foram adotadas delimitações para os últimos cinco anos, de 2021 a 2025, além dos filtros avançados de citações o *Web of Science* contemplou (*Malware Detection, Intrusion Detection, Cyber Defense, Cryptographic Protocols, Smart Grid Security, Cryptographic Hardware, Differential Privacy e Digital Privacy*) e *IEEE Xplore* contemplou (*Malware, Distributed Denial Of Service, Denial Of Service Intrusion, Detection*

SystemIntrusion, DetectionTypes, Of AttacksAnomaly, Detection,Attack Detection, Cybercrime Information, Security, Ransomware).

Tabela 1 – Termos para pesquisa avançada

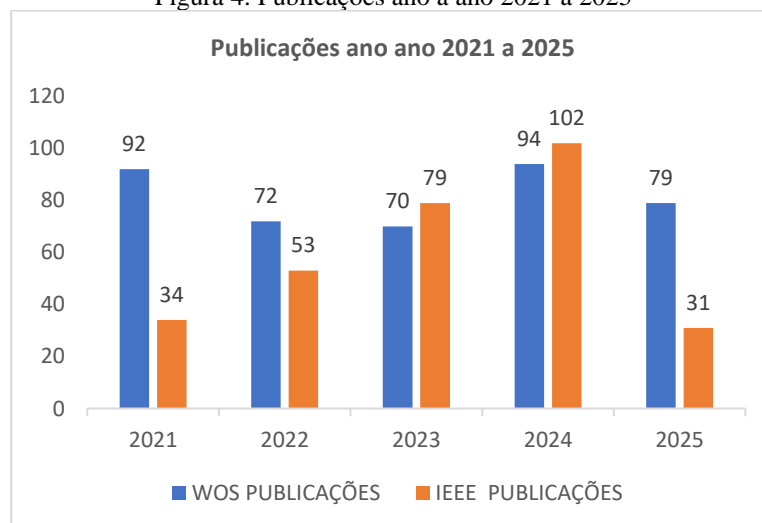
Base de Dados	Termos da Pesquisa	Resultados
Web of Science	("phishing" OR "ransomware" OR "DDoS" OR "malware") AND ("higher education" OR "universities" OR "higher education institutions" OR "instituições de ensino superior" OR "TEMAc")	400
IEEE Xplore	("phishing" OR "ransomware" OR "DDoS" OR "malware") AND ("higher education" OR "universities" OR "higher education institutions" OR "instituições de ensino superior" OR "TEMAc")	355

Fonte: Banco de Dados WoS e IEEE (2021 a 2025)

4.2 ETAPA II - APRESENTAÇÃO E CORRELAÇÃO DE DADOS

Nesta etapa realizamos a verificação das duplicatas dos dados colhidos. A soma dos bancos de dados da Web of Science e IEEE Xplore totalizam 755 artigos que serviram de amostra para o trabalho. Foram removidos 49 documentos duplicados finalizando as amostras com total de 706 registros válidos para a pesquisa. A Figura 4 mais adiante demonstra os resultados das publicações do WoS e IEEE.

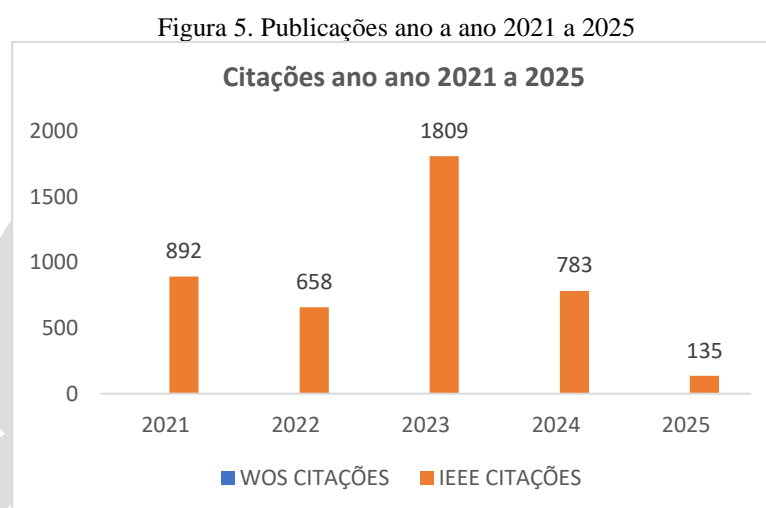
Figura 4. Publicações ano a ano 2021 a 2025



Fonte: Elaborado pelos Autores (2026)

Ao realizar a o cruzamento das duas bases de dados WoS e IEEE observou-se que os cinco artigos científicos mais citados foram: (Zili, L. et al, 2024) com 258 citações, (Bilal, H. et al, 2021) com 253 citações, (Nguyet, Q. et al, 2022) com 240 citações , (Yitong, R. et al, 2023) com 194 citações e (Kai, P. et al, 2021) com 149 citações.

Os quantitativos de citações mencionadas foram obtidos através da inserção dos títulos dos artigos na barra de buscas do Google Scholar. A Figura 5 mais adiante demonstra os resultados das citações do WoS e IEEE.



Fonte: Elaborado pelos Autores (2026)

Através das bases de dados analisadas, verificou-se que, nos últimos cinco anos, 54 países que apresentaram publicações relacionadas ao tema, evidenciando sua relevância e alcance internacional. Na Tabela 2 estão apresentados os 10 países que mais publicaram. O Brasil divide a oitava posição empatado com a Emirados Árabes com 13 artigos, ou seja, 1,8% dos artigos publicados.

Tabela 2 – Número de publicações por país

Países	Publicações	%
China	238	33,7 %
India	107	15,0 %
USA	99	14,0 %
Italy	26	3,7 %
Saudi Arabia	24	3,4 %
France	23	3,3 %
Japan	15	2,1 %
Brazil	13	1,8 %
UArabEmirates	13	1,8 %

Spain	11	1,6 %
Outros	137	19,4 %
Total	706	100

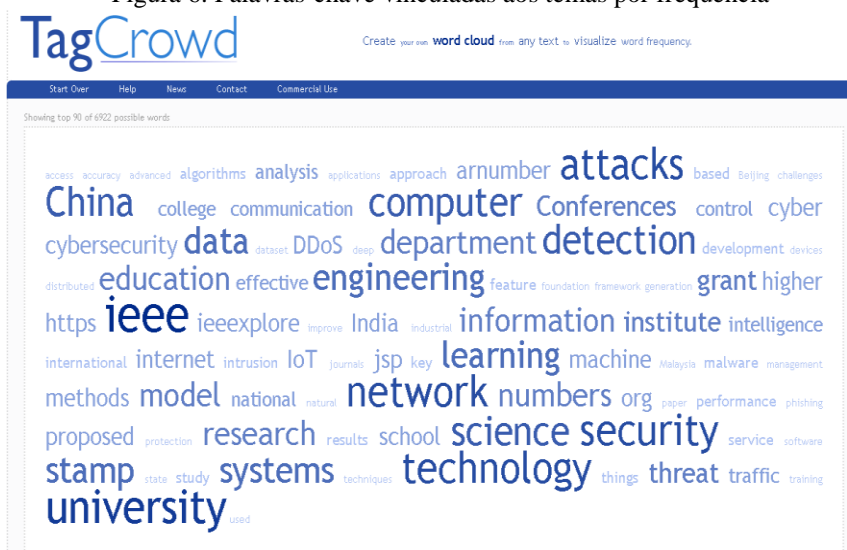
Fonte: Banco de Dados WoS e IEEE (2021 a 2025)

Os demais países possuem um percentual abaixo de 1,6 das publicações, ou seja, abaixo de 11 artigos publicados e como foram inferiores foram aglutinados como outros.

Em relação aos dados de pesquisas do Brasil foram encontrados treze publicações acadêmicas dentre elas cinco pesquisas das treze forma as que mais se destacaram em relação as citações e são eles: Previsão de ataques distribuídos de negação de serviço: desafios, questões em aberto e oportunidades (de Neira, A.et al, 2023) com 61 citações, Rápido e furioso: sobre a modelagem da detecção de malware como um fluxo de dados em evolução (Ceschin, F. et al, 2023) com 32 citações, Estrutura baseada em tensores para detecção de ataques distribuídos de negação de serviço (Maranhão, JPA. et al, 2021) com 15 citações, Um sistema inteligente para previsão de ataques DDoS com base em sinais de alerta precoce (de Neira,A.et al, 2023) com 11 citações, e a Abordagem de engenharia de recursos não supervisionada para prever ataques DDoS (de Neira,A.et al, 2023) com 3 citações.

Em relação a frequência de palavras-chave dos artigos da WoS e IEEE concatenados, as amostras selecionadas são apresentadas na Figura 6. Para obter a “nuvem de palavras”, foi utilizada a ferramenta *TagCrowd*, que monta um diagrama com as palavras colocando em destaque as palavras mais observadas através dos dados inseridos no *software*. (TagCrowd, 2022).

Figura 6. Palavras-chave vinculadas aos temas por frequência



Fonte: (TagCrowd, 2022).

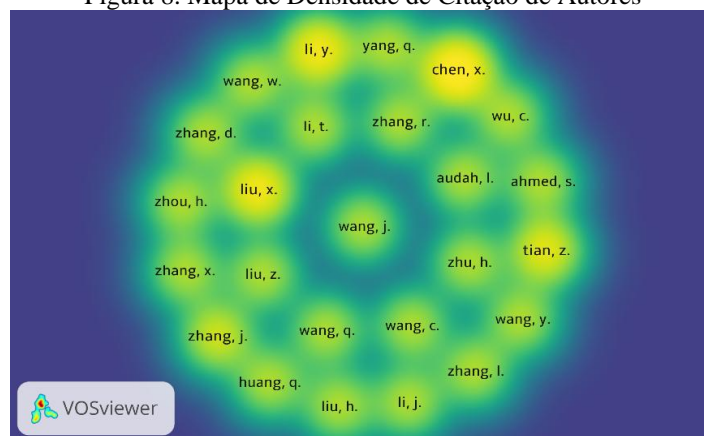
4.3 ETAPA III - APROFUNDAMENTO, MODELO DE INTEGRAÇÃO E VALIDAÇÃO POR MEIO DE DADOS POR EVIDÊNCIAS

Na etapa III realizou-se a inter-relação dos metadados, aprofundando, o modelo de integração e validação por meio de dados por evidências, para chegar a mais este resultado executou-se o mapeamento científico tendo como auxílio o *software* chamado *VosViewer* (VosViewer, 2022).

O mapeamento teve como base os metadados extraídos das bases do WoS e IEEE aglutinados entre si. A ideia do mapa de visualização de densidade é identificar ou entender como os trabalhos científicos se relacionam (VosViewer, 2022). Nos mapas, são utilizadas cores mais intensas (vivas) e fontes em destaques para evidenciar os itens que apresentam maior frequência de associação. Os que se relacionam com pouca intensidade são representados com tonalidades mais suaves e fontes reduzidas.

Avançando na análise do mapa de densidade de co-autoria este determinará com base nos números de documentos que os autores publicaram em colaboração. Para executar esta tarefa foram filtrados apenas os autores que publicaram pelo menos 2 artigos científicos. Segue abaixo a Figura 7 do mapa de densidade (VosViewer, 2022).

Figura 8. Mapa de Densidade de Citação de Autores



Fonte: Wang.J (2023)

4.4 DA PESQUISA REALIZADA: DETECÇÃO DE MALWERES COMO PHISHING, RANSOMWARE E TÉCNICAS DE ATAQUES ATRAVÉS DO DDOS.

Após análise sistemática da literatura o tema abordado possui uma importância científica de extrema relevância e segue respaldada por um volume expressivo de bibliografias relevantes. Cabe reforçar que a proteção dos dados em uma instituição de ensino superior é importante em razão do exponencial volume de dados científicos armazenado. Esses problemas podem ser solucionados ou/e minimizados com auxílio das seguintes propostas:

- a) Um método automático e eficiente de classificação de tráfego de malware para uma Internet das Coisas segura (Zhang, X. *et al* 2024);
- b) Fortalecendo a segurança de rede com switches programáveis: uma pesquisa abrangente (Xiang, C. *et al* 2023);
- c) Aprendizado profundo para detecção de phishing: taxonomia, desafios atuais e direções futuras (Nguyet Qaunt, D. *et al* 2022);
- d) A ascensão do ransomware: uma análise de ataques, técnicas de detecção e desafios futuros (Kamil, S. *et al* 2022);
- e) Previsão de ataques distribuídos de negação de serviço: desafios, questões em aberto e oportunidades (de Neira,A.*et al*, 2023);
- f) Um sistema inteligente para previsão de ataques DDoS com base em sinais de alerta precoce (de Neira,A.*et al*, 2023);

g) Abordagem de engenharia de recursos não supervisionada para prever ataques DDoS (de Neira, A. et al, 2023).

O primeiro problema pode ser mitigado através do Método Automático e Eficiente de Classificação de Tráfego de Malware para Internet das Coisas Seguras. Segundo os autores, a classificação de *malware* é de suma importância para a segurança cibernética, entretanto apresenta elevada complexidade. Os resultados obtidos do sistema automático com arquitetura neural proposto, mostrou que o método MTC auxiliado pelo NASP pode alcançar um desempenho ideal no gerenciamento da rede para a Internet das Coisas (IoT) (Zhang, X. et al 2024).

O artigo Fortalecimento da Segurança de rede com *Switches* programáveis destaca que, como avanço das tecnologias de redes 5G e da inteligência artificial os ataques de negação de serviço (DDoS) se tornaram mais comuns. Diante do cenário, os autores analisaram que o uso de *Switches* Programáveis, seria um facilitador de técnicas avançadas que motivaria implementações mais seguras. (Xiang, C. et al 2023).

Já o artigo Aprendizado Profundo para Detecção de *Phishing*: Taxonomia, Desafios Atuais e Direções Futuras, os autores evidenciam a preocupação com os ataques de *Phishing* apontando que muitas técnicas apesar de sofisticadas apresentam limitações de desempenho e precisão. O trabalho propõe uma taxonomia de algoritmos baseada em uma revisão sistemática que contou com 81 referências (Nguyet Quant, D. et al 2022).

O artigo A Ascensão do Ransomware: Análise de Ataques, Técnicas de Detecção e Desafios Futuros, aborda a segurança da informação como um tema urgente. Os autores enfatizam que, apesar dos avanços nos sistemas de proteção, invasões bem-sucedidas de *ransomware* continuam sendo um dos maiores desafios, pois uma vez que o atacante criptografa os dados da vítima causando impactos e transtornos ainda solicita o pagamento de um resgate pelos dados capturados de forma ilícita. (Kamil, S. et al 2022).

No artigo Previsão de Ataques Distribuídos de Negação de Serviço: Desafios, Questões em Aberto e Oportunidades, os autores classificam os ataques de DDoS como uma das principais ameaças cibernéticas da atualidade. O estudo aponta que mudanças de comportamentos no cenário pós-pandemia da COVID-19 tornaram as medidas menos eficazes, principalmente devido aos múltiplos vetores de ataque utilizados pelos cibercriminosos que consomem largura de banda e exploram limitações dos protocolos de rede (de Neira, A. et al, 2023).

Outro trabalho de extrema relevância é o Sistema Inteligente para Previsão de Ataques DDoS com Base em Sinais de Alerta Precoce, no qual os autores propõem um sistema cooperativo denominado COOPRED DDoS. Apesar da sofisticação dos ataques cibernéticos, os resultados demonstram que o sistema é capaz de prever ataques com até 3 minutos e 49 segundos de antecedência, alcançando taxas de precisão entre 99,60% e 99,87% evidenciando a eficácia de abordagens preditivas e preventivas (de Neira, A. *et al*, 2023).

Por fim, o último artigo trata da Abordagem de Engenharia de Recursos não Supervisionada para Prever Ataques DDoS enfatizando a importância da previsão antecipada, especialmente em ambientes de IoT. A abordagem de engenharia de recursos não supervisionada (SEE) possibilitou a previsão do ataque com 30 minutos antes de sua ocorrência, avançando índices de 100% (de Neira, A. *et al*, 2023).

5 CONCLUSÃO

O artigo científico analisou as principais obras publicadas referenciadas pela detecção de *malwares* como *phishing* e *ransomware* e a técnica de ataque do DDoS a instituições de ensino superior. A pesquisa foi realizada com auxílio da Teoria do Enfoque Metaanalítico Consolidado (TEMAC), dentre os anos de 2021 a 2025. O estudo foi sustentado pelos principais autores na área pesquisada que foram essências para a conclusão deste documento acadêmico.

Após a investigação dos resultados, observou-se que cinco artigos científicos mais citados foram: (Zili, L. *et al*, 2024) com 258 citações, (Bilal, H. *et al*, 2021) com 253 citações, (Nguyet, Q. *et al*, 2022) com 240 citações, (Yitong, R. *et al*, 2023) com 194 citações e (Kai, P. *et al*, 2021) com 149 citações.

Entretanto as informações levantadas evidenciam que boa parte das obras publicadas se concentram na detecção de *malwares*, com destaque para ameaças de *phishing* e *ransomware* e técnicas de ataque do DDoS no contexto das instituições de ensino superior. O estudo reforça a preocupação do setor acadêmico com a segurança cibernética que são capazes de comprometer a integridade dos dados e a funcionalidade das atividades institucionais.

Em relação a mitigação dos problemas de intrusão sete artigos publicados se mostraram eficientes e foram descritos pelos autores: (Zhang, X. *et al* 2024), (Xiang, C. *et al* 2023), (Nguyet Qaunt, D. *et al* 2022), (Kamil, S. *et al* 2022) e o demais escritos por (de Neira, A. *et al*, 2023).

Eles se mostraram assuntos interessantes como classificação de tráfegos de *malware* para internet das coisas, a segurança da rede através de switches programáveis, o aprendizado profundo para a detecção de *phishing*, a detecção e desafios em relação aos ataques de *ransomware*, a previsão de ataque de DDoS, a utilização de sistemas inteligentes para alertar precocemente um ataque de DDoS e finalmente recursos de engenharia não supervisionada para alertar alerta ataques precoces.

Os resultados das análises realizadas demonstram que este artigo pode servir como pesquisas futuras relacionadas aos ataques direcionados as instituições de ensino superior, bem como instituições públicas e privadas. As evidências apresentadas contribuem para a compreensão das ameaças cibernéticas e informam os melhores caminhos para a prevenção, mitigação, detecção e resposta aos incidentes.



REFERÊNCIAS

ADRIAANSE, L.S.; RENSLEIGH, C. **A Content Comprehensiveness Comparison**. Web of Science, Scopus and Google Scholar 2011. Disponível em: <https://www.researchgate.net/publication/259258650_Web_of_Science_Scopus_and_Google_Scholar_A_content_comprehensiveness_comparison>. Acesso em: 14 nov. 2025.

BILAL, H. *et al.* **Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System Over 5G Network**. IEEE. 2020. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/9716113>> Acesso em: 21 nov. 2025.

CESCHIN, F. *et al.* **Fast & Furious: On the modelling of malware detection as an evolving data stream**. Elsevier Scopus 2022. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S0957417422016463>> Acesso em: 25 nov. 2025.

CHENG, C. K. E.; WANG, T. **Institutional Strategies for Cybersecurity in Higher Education Institutions**. MDPI: Information 9 versões 2022. Disponível em: <<https://www.mdpi.com/2078-2489/13/4/192>>. Acesso em: 12 nov. 2025.

DE NEIRA, A. B. *et al.* **An Intelligent System for DDoS Attack Prediction Based on Early Warning Signals**. IEEE 2023. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/10261168?signout=success>>. Acesso em: 09 nov. 2025.

DE NEIRA, A. B. *et al.* **Unsupervised Feature Engineering Approach to Predict DDoS Attacks**. 2023. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/10437029>> Acesso em: 14 nov. 2025.

DE NEIRA, A. B. *et al.* **Distributed denial of service attack prediction: Challenges, open issues and opportunities** ELSEVIER 2023. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S1389128622005874>> Acesso em: 16 nov. 2025.

DOLLIVER, D., S. *et al.* **Building a robust cyberthreat profile for institutions of higher education: An empirical analysis of external cyberattacks against a large university's computer network**. Elsevier Scopus. 2 versões 2021. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S175606162100029X>>. Acesso em: 16 nov. 2025.

FAN, C. *et al.* **Detection Of Ddos Attacks In Software Defined Networking Using Entropy**. MDPI. 7 versões 2021. Disponível em: <<https://doi.org/10.3390/app12010370>>. Acesso em: 16 nov. 2025.

FERREIRA, L. V. A. *et al.* **Uso de honeypots na detecção de rootkits de malware: proposta de uma agenda de pesquisa**. RISTI. 3 versões 2023. Disponível em: <https://www.researchgate.net/publication/373439857_Uso_de_honeypots_na_deteccao_de_rootkits_de_malware_proposta_de_uma_agenda_de_pesquisa>. Acesso em: 02 out. 2025

KAI, P. *et al.* **Security challenges and opportunities for smart contracts in Internet of Things: A survey**. IEEE 2022 Disponível em: <<https://ieeexplore.ieee.org/abstract/document/9409120>>. Acesso em: 21 nov. 2025.

KAMIL, S. *et al.* **The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges.** 2022. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/9759000>> Acesso em: 10 nov. 2025.

LACHI, A. A.; ANATOLIE, A.. **Cybersecurity Threat Analysis In Higher Education Institutions As A Result Of Distance Learning.** Instrumentaul Bibliometric Nacional.p. 128-133, 2022. 6 versões. Disponível em: <https://ibn.idsi.md/vizualizare_articol/163773>Acesso em: 16 nov. 2025.

LACHI, A. A. **Network Security Threats to Higher Education Institutions.** Instrumentaul Bibliometric Nacional. p. 323-333. 2021 7 versões 2022. Disponível em: < https://ibn.idsi.md/vizualizare_articol/132828 >. Acesso em: 15 nov. 2025.

LALLIE, H. S.. *et al.* **Understanding Cyber Threats Against the Universities, Colleges, and Schools.** Cornell University 3versões. 2021. Disponível em : <<https://arxiv.org/abs/2307.07755>> Acesso em: 15 nov. 2025.

MA HAQUE, Md. *et al.* **Cybersecurity In Universities: An Evaluation Model.** SN **Computer Science.** 4 versões 2023. Disponível em: <<https://link.springer.com/article/10.1007/s42979-023-01984-x> >Acesso em: 16 nov. 2025.

MARANHÃO, J. P.A. *et al.* **Tensor based framework for Distributed Denial of Service attack detection.** Elsevier Scopus 2021. Disponível em:<<https://www.sciencedirect.com/Science/article/abs/pii/S1084804520303556>> . Acesso em: 16 out. 2025.

MARIANO, A. M ; ROCHA, M. S. **Revisão da Literatura: Apresentação de uma Abordagem Integradora.**” XXVI Congresso Internacional de la Academia Europea de Dirección y Economía de la Empresa (AEDEM), 2 versões p. 427–443, n. Setembro 2017.

NAAGAS, M.A. *et al.* **Defense-Through-Deception Network Security Model: Securing University Campus Network From Dos/Ddos Attack.** Bulletin of Electrical Engineering and Informatics (BEEI). p.593-600, 14 versões 2018. Disponível em:<<https://beei.Org/index.php/EEI/article/view/1349> > Acesso em: 16 nov. 2025.

NASCIMENTO, L. M. M. *et al.* **Aumentando a Segurança do Gerenciamento de Usuários do Moodle Usando Banco de Dados de Terceiros.** 2025. Revista de Engenharia e Tecnologia. Disponível em: <<https://revistas.uepg.br/index.php/ret/article/view/25201>>. Acesso em: 28 dez. 2025.

NEVES, R.A.C. **Vitimação Por Phishing: Um Estudo Empírico.** Proquest 2022. Disponível em:<<https://www.proquest.com/openview/0b3450e6e7eebbe6ece34ad794b54ce8/1?pq-origsite=gscholar&cbl=2026366&diss=y>>Acesso em: 08 nov. 2025.

NGUYET, Q. D., *et al.* **Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions** IEEE 2022. Disponível em: < <https://ieeexplore.ieee.org/abstract/document/9716113> >Acesso em: 16 nov. 2025.

PILLAY, A.; SHARMA, N. A. **Applicable cyber security commendations to prevent cyber attacks in Universities.** IEEE.2023. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/10089360> > Acesso em: 09 nov. 2025.

RAJPUT, P. H. N.. *et al.* **Remote Non-Intrusive Malware Detection for PLCs based on Chain of Trust Rooted in Hardware.** IEEE European Symposium on Security and Privacy (EuroS&P), p.369-384. 5 versões 2021. Disponível em: <<https://ieeexplore.ieee.org/document/9581272>>. Acesso em: 15 nov. 2025.

STEINBOCK, D. D. (2022). **TagCrowd.** Disponível em: <https://tagcrowd.com/>. Acesso em: 08 nov. 2025.

ULVEN, Joachim Bjørge, WANGEN, Gaute. **A Systematic Review of Cybersecurity Risks in Higher Education.** MDPI: Future Internet . 7 versões. 2021. Disponível em: <<https://www.mdpi.com/1999-5903/13/2/39>> .Acesso em: 11 nov. 2025.

WANG, J *et al.* **Visualizing the Landscape of Home IoT Research: A Bibliometric Analysis UsingVOSviewer.**MDPI 2023.Disponível em:<<https://www.mdpi.com/1424-8220/23/6/3086>> Acesso em: 08 nov. 2025.

XIANG, C. *et al.* **Empowering Network Security With Programmable Switches: A Comprehensive Survey.** IEEE 2023. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/10098550> > Acesso em: 21 nov. 2025.

YITONG, R. L *et al.* **CSKG4APT: A Cybersecurity Knowledge Graph for Advanced Persistent Threat Organization Attribution.**2022. Disponível em: <https://www.ijesat.com/ijesat/files/V23I107_1696484982.pdf >. Acesso em: 21 nov. 2025.

ZHANG, X. *et al.* **An Automatic and Efficient Malware Traffic Classification Method for Secure Internet of Things.** 2023. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/10261168?signout=success>>. Acesso em: 09 nov. 2025.

ZILI, L. *et al.* **Federated Learning With Non-IID Data: A Survey.** IEEE 2024. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/10468591> >. Acesso em: 21 nov. 2025.