SEGURANÇA DIGITAL: ATAQUES CIBERNÉTICOS MAIS COMUNS EM REDES

Samuel de Macedo Lins[1], Credson Isaac[1], Diego da Silva Pereira[1]

[1]Laboratório de Pesquisa em Redes e Sistemas Computacionais (NOCS LAB), Instituto Federal do Rio Grande do Norte, Parnamirim, Brasil (samuel.lins@escolar.ifrn.edu.br)

Resumo: Este trabalho analisa a segurança digital, focando nos ataques cibernéticos mais frequentes em redes: Phishing e Malware. O objetivo é descrever essas ameaças e formas de mitigação. Por meio de pesquisa acadêmica, discutem-se as vulnerabilidades e a importância de medidas preventivas para a proteção de dados. Portanto, o investimento em cibersegurança e a conscientização dos usuários são fundamentais para garantir a integridade das informações em ambientes de rede atuais.

Palavras-chave: Segurança Digital; Ataques Cibernéticos; Redes de Computadores; Vulnerabilidades; Cibersegurança.

1. INTRODUÇÃO

A expansão acelerada das redes de computadores e a crescente dependência da sociedade por serviços digitais transformaram a conectividade em um pilar fundamental da infraestrutura moderna. No entanto, essa evolução tecnológica trouxe consigo um aumento proporcional nas vulnerabilidades, tornando a segurança digital um dos maiores desafios contemporâneos para organizações e usuários comuns.

Dentro da área de Redes, ataques como phishing e de malwares têm se destacado pela sua frequência e capacidade de impacto. Com isso, a exploração de falhas em protocolos de rede e o uso de engenharia social são as portas de entrada mais comuns para incidentes de segurança. E, para a mitigação de tais ocorrências de forma mais eficaz, é necessário que o profissional da área de tecnologia compreenda não apenas as ferramentas de defesa, mas também o comportamento dos atacantes.

Diante deste cenário, o contexto deste artigo insere-se na necessidade de identificar os padrões de ataque mais recorrentes no ambiente de redes atual, com o objetivo de analisar os ataques cibernéticos mais comuns em redes de computadores, descrevendo suas formas de funcionamento, impactos, casos reais e principais medidas de prevenção.

2. MATERIAL E MÉTODOS

Engloba a consulta a artigos científicos, sites e materiais acadêmicos sobre segurança em redes e notícias de casos reais de ataques cibernéticos.

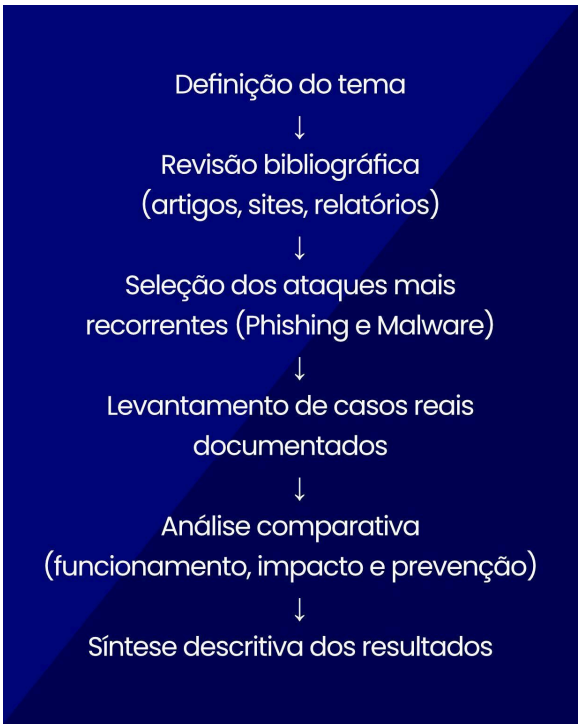

Figura 1. Fluxo metodológico.

3. RESULTADOS E DISCUSSÃO

3.1 PHISHING

O phishing, com suas primeiras aparições na década de 1990, é um tipo de ataque que usa e-mails, SMS/mensagens de texto, ligações telefônicas, sites ou redes WI-FI fraudulentas para enganar as pessoas para roubar seus dados pessoais e/ou infectar seus dispositivos com malware de maneira maliciosa, podendo ter total controle sobre a máquina da vítima.

Sob esse viés, é um tipo de engenharia social que "pesca" as pessoas de uma maneira atraente, ou seja, utiliza-se de erros humanos, histórias falsas e táticas de pressão para a manipulação mental e emocional. Ou seja, essa forma de ataque explora vulnerabilidades humanas mais do que falhas tecnológicas. Muitos criminosos utilizam mensagens que geram senso de urgência ou medo para induzir decisões rápidas sem verificação adequada da autenticidade da informação. De acordo com o Relatório do custo das violações de dados da IBM (2025), o phishing é o vetor de violação de dados mais comum existente, representando 15% de todas as violações globais. Esse tipo de ataque custa às organizações em média US$4,88 milhões de prejuízo.

Nesse contexto, em ambientes corporativos, o phishing é frequentemente utilizado para obter credenciais de acesso à rede, como usuários e senhas de e-mail institucional, VPNs, sistemas internos e serviços de autenticação. Uma vez em posse dessas informações, o atacante pode acessar recursos da rede sem autorização, comprometendo a confidencialidade e a integridade dos dados. Dessa maneira, além do roubo de informações, o phishing é frequentemente utilizado como vetor inicial para a disseminação de malwares que será discutida na próxima seção deste trabalho.

Figura 2. 88% das organizações sofreram pelo menos um ataque de phishing em 2021.

Em 2016, hackers russos usaram um e-mail falso que simulava um alerta de segurança de redefinição de senha do Google para o chefe da campanha de Hillary Clinton, candidata à presidência, e para outros membros da equipe dela. Com isso, milhares de e-mails foram roubados e divulgados na internet contra a candidata. (Mike Vizard, 2019).

Para se prevenir contra o phishing, é preciso sempre usar o bom senso antes de fornecer dados sensíveis na internet. O usuário nunca deve confiar em mensagens alarmantes (urgência) na caixa de entrada de SMS, telefone ou em redes sociais, em links incorporados e anexos suspeitos em e-mails. Manter seu navegador e sistema operacional constantemente atualizados é crucial para aumentar a segurança. Além disso, os usuários devem evitar responder mensagens suspeitas ou de spam, pois essa interação pode confirmar ao cibercriminoso que o endereço eletrônico ou número telefônico está ativo, aumentando a probabilidade de novos ataques.

Em ambientes corporativos e institucionais, a prevenção também depende da implementação de mecanismos de segurança em rede. Soluções como filtros antispam e firewalls, auxiliam na identificação e no bloqueio de tentativas de phishing antes que alcancem os usuários. Adicionalmente, o monitoramento do tráfego de rede pode reduzir os impactos causados pelo comprometimento de credenciais obtidas por meio desses ataques.

3.2 MALWARE

O malware é um software, código ou programa malicioso feito para infectar e causar danos em redes, computadores e dispositivos móveis. Surgiu em 1966 como um modelo conceitual de um programa que poderia se reproduzir e se espalhar por um sistema. Nesse viés, ele tem o poder de danificar um dispositivo, coletar informações ou ser usado para extorquir dinheiro da vítima, infiltrando-se sem o seu consentimento. Alguns se espalham explorando vulnerabilidades em softwares em execução na máquina ou os invasores enganam as vítimas para que instalem software malicioso em seus computadores. Com isso, uma vez que um malware é instalado no dispositivo ou na rede da vítima, ele pode fazer o que foi projetado para fazer: criptografar ou excluir arquivos, espionar e controlar a máquina do usuário, roubar dados pessoais, fazer sequestro de DNS (manipulação e redirecionamento do endereço de sites) e aplicar outros ataques.

De acordo com o engenheiro de segurança da informação Rishabh Goyal (2026), são detectados mais de 560.000 novos malwares diariamente e a cada minuto, quatro empresas são vítimas de ataques de ransomware (um tipo de malware que sequestra arquivos e dados do dispositivo da vítima, os criptografando, e só os devolve novamente quando é pago o valor exigido).

Em 12 de maio de 2017, o ransomware WannaCry infectou e se espalhou para mais de 200 mil computadores em mais de 150 países. Ele criptografou e inutilizou os computadores infectados, exigindo inicialmente US$300, que posteriormente subiu para US$600 ao longo dos dias. Com isso, estimou-se um prejuízo global de cerca de US$ 4 bilhões. Empresas grandes como FedEx, Honda, Nissan e o Serviço Nacional de Saúde (NHS) do Reino Unido foram muito afetadas pelo ataque.

Figura 3. Tela do Ransomware WannaCry.

Para se proteger de malwares, é recomendável ao usuário sempre manter o sistema operacional e softwares atualizados, pois as atualizações corrigem falhas de segurança que podem ser exploradas por malwares. Nesse contexto, os antivírus são muito importantes para a segurança digital, pois são ferramentas de proteção que identificam, bloqueiam e removem ameaças reconhecidas por eles. Eles devem ser constantemente atualizados e mantidos no modo de proteção em tempo real. Além disso, utilizar firewall é extremamente importante, pois ele é responsável por ser uma barreira de segurança digital que monitora e filtra o tráfego de dados entre o seu dispositivo ou rede e a internet, ou seja, ele bloqueia ameaças e permite apenas a entrada e saída de informações confiáveis com base em regras predefinidas.

O usuário precisa ter boas práticas na internet, como evitar clicar e baixar arquivos de fontes, sites e aplicativos desconhecidos, utilizar senhas fortes e autenticação de dois fatores.

As redes Wi-Fi representam um dos principais pontos de acesso às infraestruturas computacionais modernas. Devido à transmissão sem fio dos dados, tornam-se alvos frequentes de ataques cibernéticos, como interceptação de tráfego, acesso não autorizado e criação de redes falsas. Dessa forma, para a segurança da rede, é recomendável utilizar protocolos de proteção que criptografam a comunicação entre os dispositivos da rede e o roteador, como o WPA2 ou WPA3. Utilizar senhas fortes, ou seja, ter mais de 12 caracteres, combinar letras, números e símbolos, não tendo dados pessoais. Atualizar o firmware do roteador para correção de falhas de segurança. E, uma boa dica para empresas e instituições é separar a rede na configuração: rede interna e outra para visitantes, pois impede que o público externo tenha acesso direto aos dados internos.

CONCLUSÃO

Esta análise demonstra que o phishing e o malware constituem as ameaças mais críticas e frequentes à segurança em redes contemporâneas, explorando tanto falhas tecnológicas quanto vulnerabilidades humanas.

Conclui-se que o phishing permanece como o principal vetor de violação de dados global, exigindo que as organizações invistam não apenas em ferramentas técnicas, como filtros antispam e firewalls, mas, fundamentalmente, na conscientização dos usuários contra táticas de engenharia social. Simultaneamente, o impacto devastador de malwares, exemplificado pelo caso WannaCry, reforça a necessidade imperativa de manter sistemas operacionais atualizados e utilizar softwares antivírus em tempo real para mitigar prejuízos bilionários .

No que tange à infraestrutura de rede, a segurança de conexões Wi-Fi por meio de protocolos robustos como WPA2 e WPA3, além da segmentação de redes internas, são estratégias essenciais para impedir acessos não autorizados.

Portanto, a garantia da integridade e confidencialidade das informações em ambientes digitais depende da convergência entre o gerenciamento técnico rigoroso da rede e a adoção de boas práticas de navegação pelos usuários.

REFERÊNCIAS

CLOUDFLARE. O que foi o ataque de ransomware WannaCry? Cloudflare, 2026. Disponível em: https://www.cloudflare.com/pt-br/learning/security/ransomware/wannacry-ransomware/. Acesso em: 23 junho 2026

GOYAL, Rishabh. Mais de 30 estatísticas sobre malware que você precisa conhecer em 2026. Astra, 2026. Disponível em: https://www.getastra.com/blog/security-audit/malware-statistics/. Acesso em: 23 junho 2026

IFRS. Guia Educativo: 10 Ataques Cibernéticos Mais Comuns. Instituto Federal do Rio Grande do Sul, Vacaria, 2025. Disponível em: https://ifrs.edu.br/vacaria/wp-content/uploads/sites/15/2025/07/GuiaEducativo10AtaquesCiberneticos.pdf. Acesso em: 25 maio 2026.

KASPERSKY. Tudo sobre prevenção e golpes de phishing: o que você precisa saber. Kaspersky Cybersecurity, 2026. Disponível em: https://www.kaspersky.com.br/resource-center/preemptive-safety/phishing-prevention-tips. Acesso em: 19 junho 2026

KOSINSKI, Matthew. O que é phishing? IBM (International Business Machines), 2024. Disponível em: https://www.ibm.com/br-pt/think/topics/phishing Acesso em: 25 maio 2026

VIZARD, Mike. O relatório Mueller detalha como o pesadelo nacional começou com uma simples campanha de spearphishing. Barracuda, 2019. Disponível em: https://blog.barracuda.com/2019/04/26/mueller-report-details-how-long-national-nightmare-started-with-simple-spearphishing-campaign. Acesso em: 17 abril 2026