Browse our categories

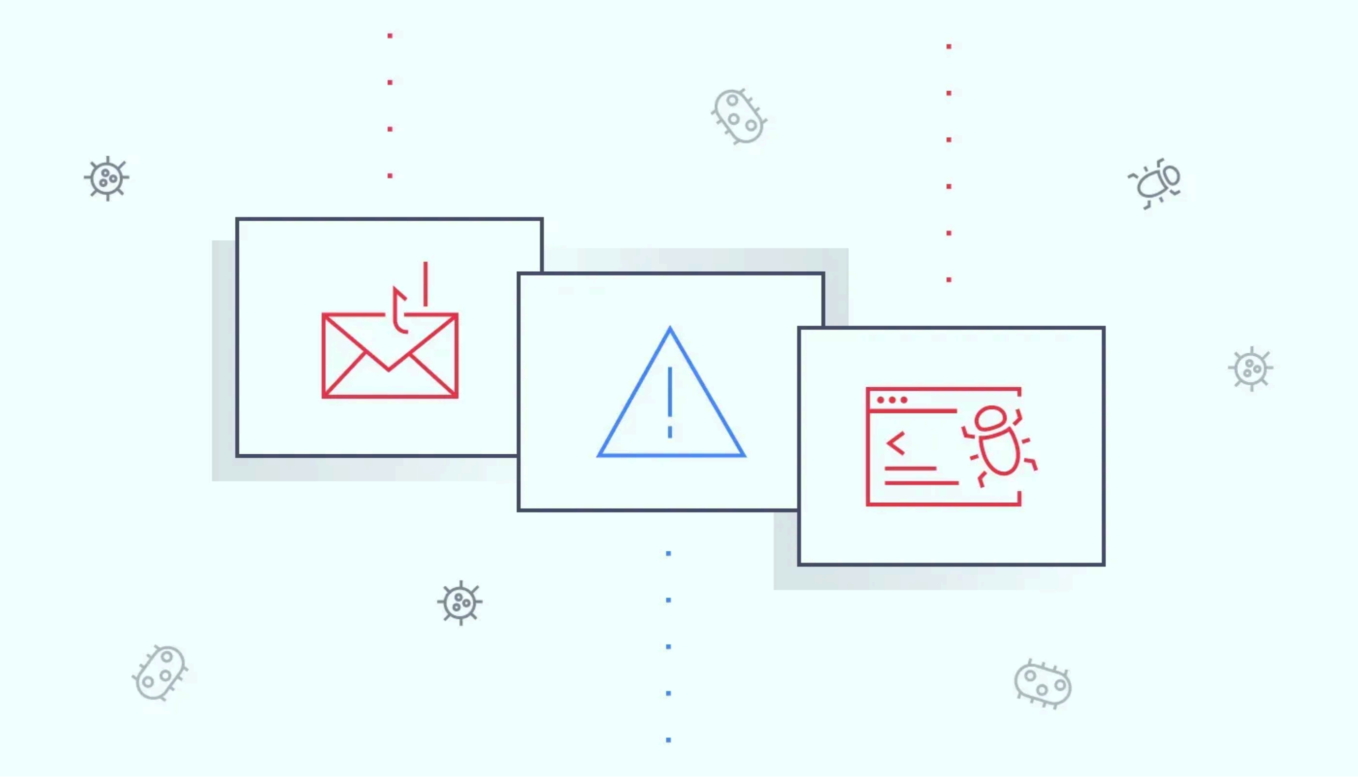
Blog / Trends & statistics

TRENDS & STATISTICS

Most common types of cyber-attacks 2024

Agnė Srėbaliūtė

Dec 2, 2024 10 min read



> ***Summary:*** *The article discusses the most common types of cyber-attacks in 2024, highlighting how cybercriminals evolve their tactics, making organizations increasingly vulnerable.*

Cybercriminals are constantly evolving their tactics, launching sophisticated attacks across various sectors. From large-scale nation-state campaigns to ransomware attacks, these cybersecurity threats continue growing in frequency and complexity, leaving individuals and organizations vulnerable.

While the core types of attacks—like phishing and ransomware—remain prevalent in 2024, they have become more advanced. Spear phishing campaigns are more targeted, and ransomware tactics now often involve double extortion.

Additionally, newer cyber threats, like DNS tunneling and zero-day exploits, are gaining prominence. Organizations must stay informed and proactive as digitalization evolves to defend against emerging and familiar cyber threats. The rise of artificial intelligence in cybersecurity has also introduced both advanced defenses and new vulnerabilities.

What is a cyber-attack?

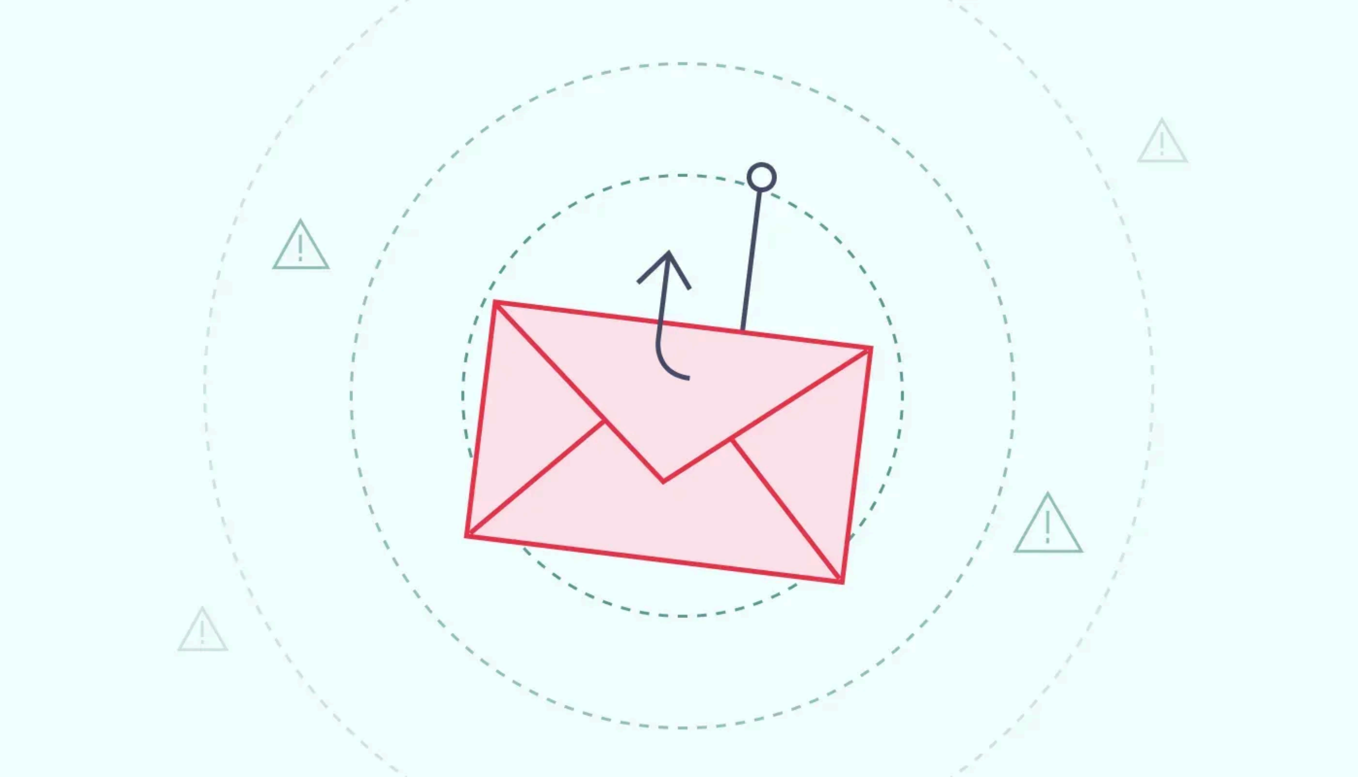
A cyber-attack is **a malicious and deliberate attempt by an individual or an organization to breach an information system**. The attacker (often called a hacker) aims to disrupt, damage, steal, alter, or gain unauthorized access to a computer system or network, usually intending to extract or compromise data.

Some cyber-attacks are financially motivated. They may target individuals, businesses, or financial institutions to steal sensitive information, resulting in data breaches. Data like credit card details, login credentials, or personal information can be sold on the black market or used for fraud.

Other types of cyber-attacks may be driven by political or strategic motives. For instance, supply chain attacks target organizations indirectly by compromising their vendors or third-party suppliers, leading to widespread damage and data breaches.

Cyber-attacks can take wildly different forms, from installing spyware on a device to conducting large-scale distributed denial of service (DDoS) on significant network infrastructure. Businesses relying on cloud security solutions must ensure they implement robust measures to mitigate these risks effectively. Here are its main types:

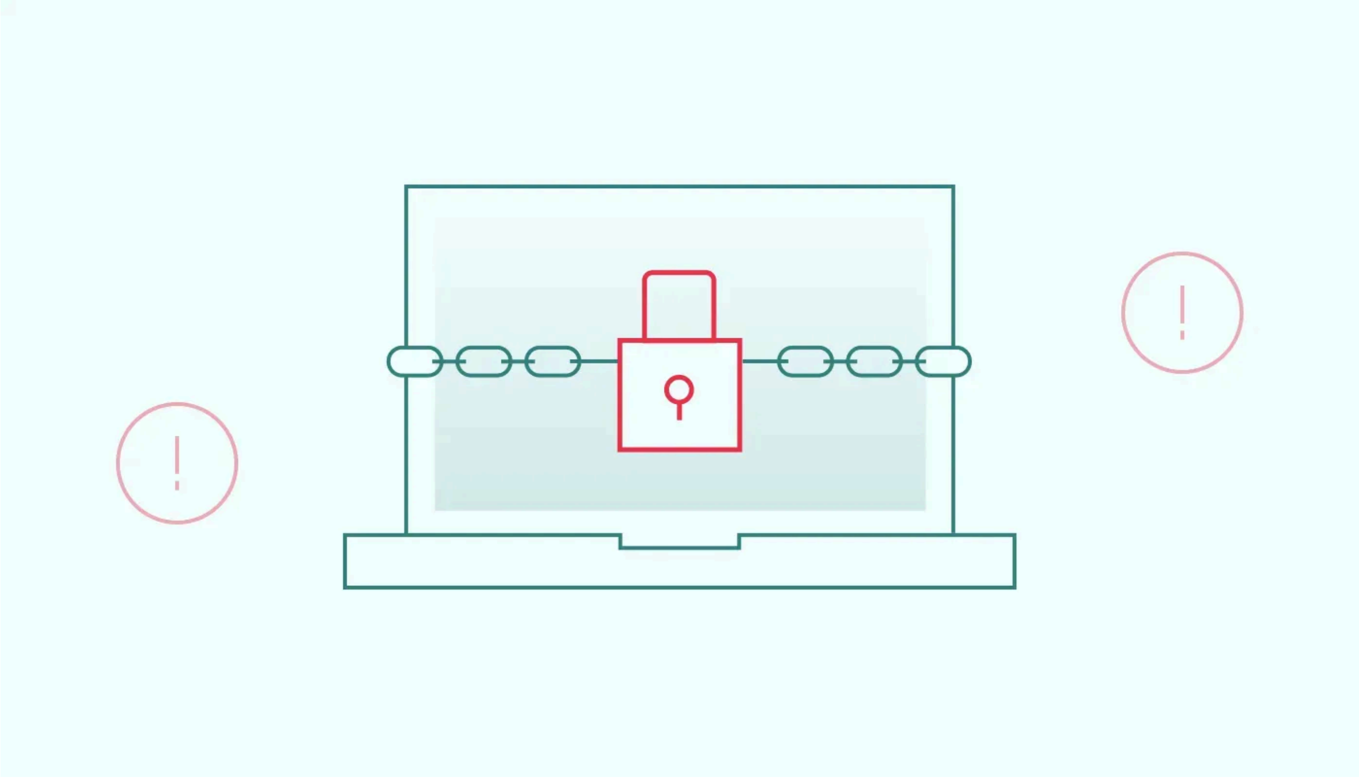
Phishing



Phishing is a social engineering tactic where attackers **impersonate trusted entities, often via email, to deceive victims into sharing sensitive information**. Phishing cyber attacks look like genuine emails from colleagues or official institutions. The catch is that the provided links in these emails lead to malicious websites or initiate malware downloads.

In real life, a phishing attack is usually a gateway to initiating additional cyber-attacks. Phishing may be used to obtain genuine user credentials to plant malware or access classified documents. As one of the most common cyber-attack methods, it primarily targets individual users and SMBs (small and medium-sized businesses).

Ransomware

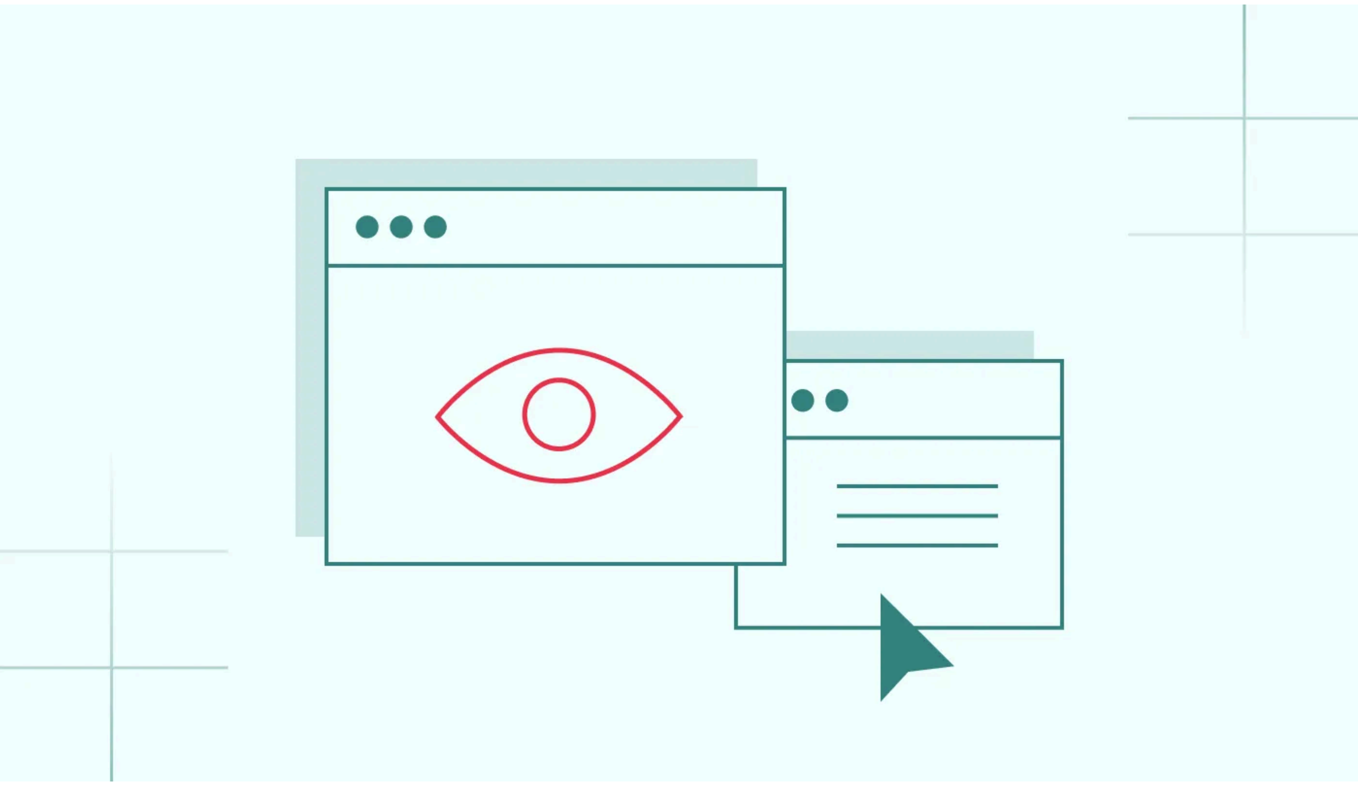


Ransomware **locks down a victim's files and demands a ransom to restore access**. This type of attack often leads to data breaches, as sensitive information may be stolen before files are encrypted. With its lucrative nature, ransomware remains one of the most significant cybersecurity threats in 2024.

With the advent of cryptocurrencies and the increasing connectivity of devices, hackers can remain anonymous while exploiting the fact that many businesses rely on cloud computing and digital technologies. One such incident can put all business operations out of commission.

High data value enables hackers to get away with a hefty ransom, as sometimes it may seem cheaper and faster to pay the amount for a business. The lucrativeness of this cyber attack type was one of the main contributing factors to its popularity in 2024.

Spyware



Spyware is another type of **malware that tracks data flowing through network assets and sends this information to controllers outside** the targeted organization. Hackers use it as a monitoring tool to track their victim's activities or extract other personal data. Spyware can include keystrokes, browsing habits, and even confidential business information.

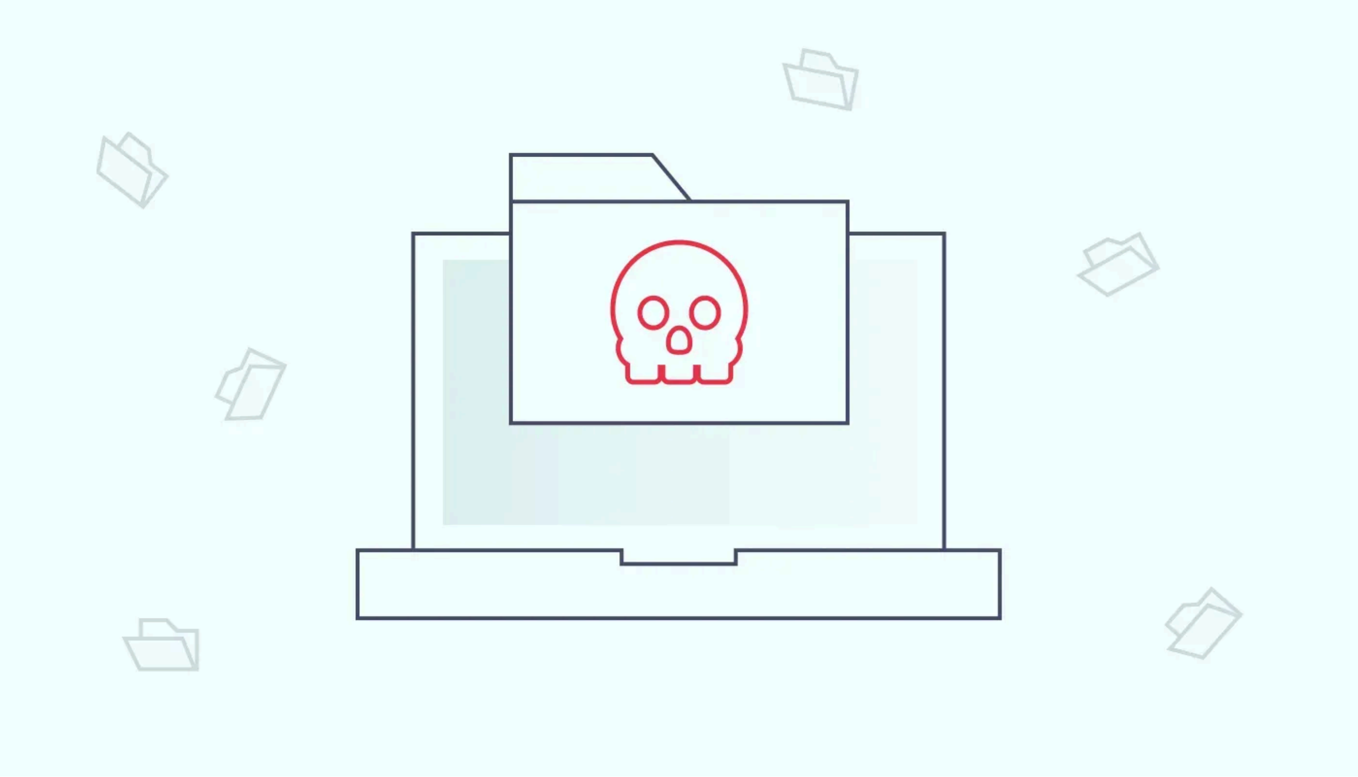
This malware can be spread through infected websites, malicious emails, hacked USB flash drives, or even freeware applications. Some advertisers even use spyware legitimately to deliver targeted ads (as most users agree to terms and conditions without actually reading them).

Viruses

Also known as worms, **viruses are self-replicating malicious software** that can quickly infect large connected networks. Their effects can range from light disruption to complete system failure. Some viruses remain dormant for long periods, while others are set to work immediately.

They work by attaching to an executable host file, which results in their viral codes executing when a file is opened, such as an Excel sheet or a .pdf document. It means that viruses generally spread through email attachments and file-sharing programs. In any case, businesses must be up to date to detect such attachments before they wreak havoc on their perimeter.

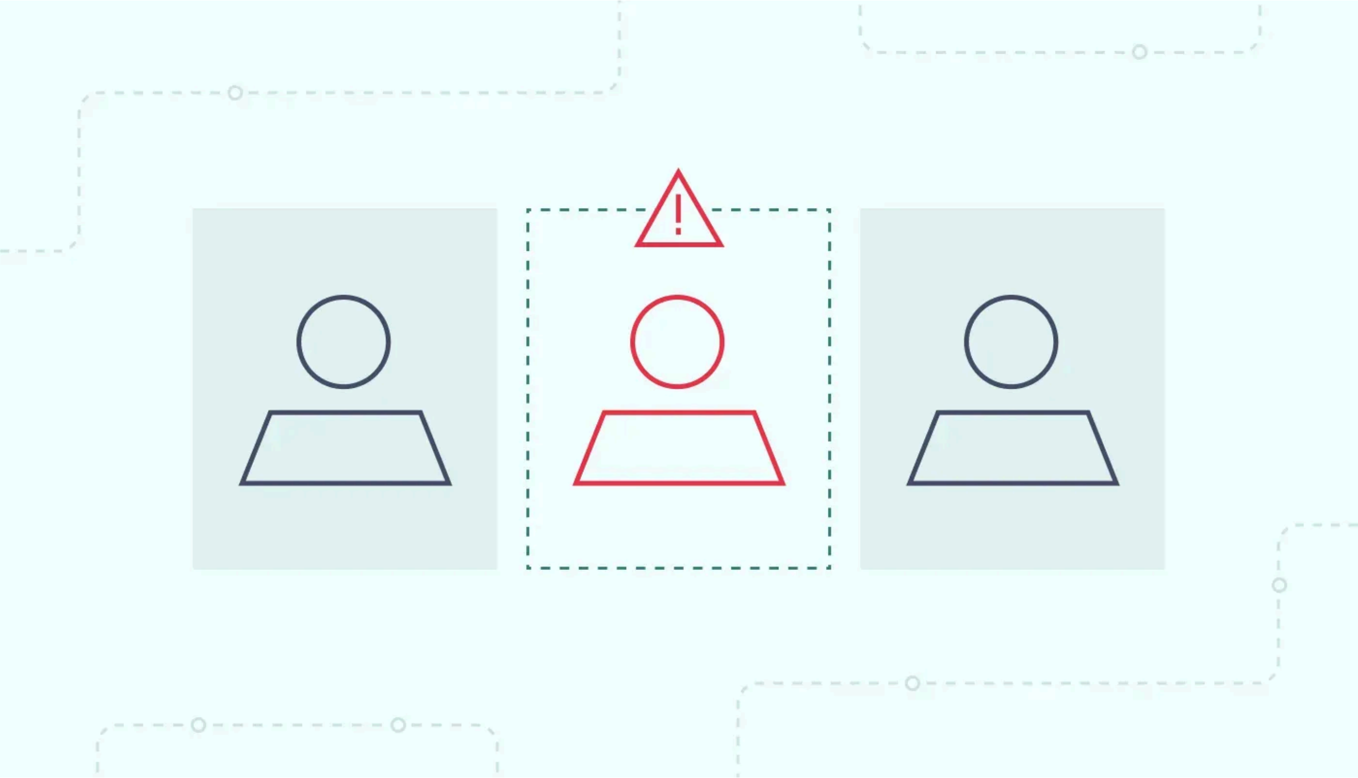
Malware



Malware encompasses **a broad category of malicious software designed to infiltrate, damage, or disrupt systems** by leaking confidential data, causing data breaches, or compromising system security. Its actions vary depending on the type—for example, viruses replicate to spread across devices, while Trojans disguise themselves as legitimate software to trick users.

Spyware secretly collects user information, and ransomware locks systems until a payment is made. Understanding these distinctions helps organizations deploy targeted defenses, such as antivirus software, real-time monitoring tools, and strict access controls, to guard against malware threats.

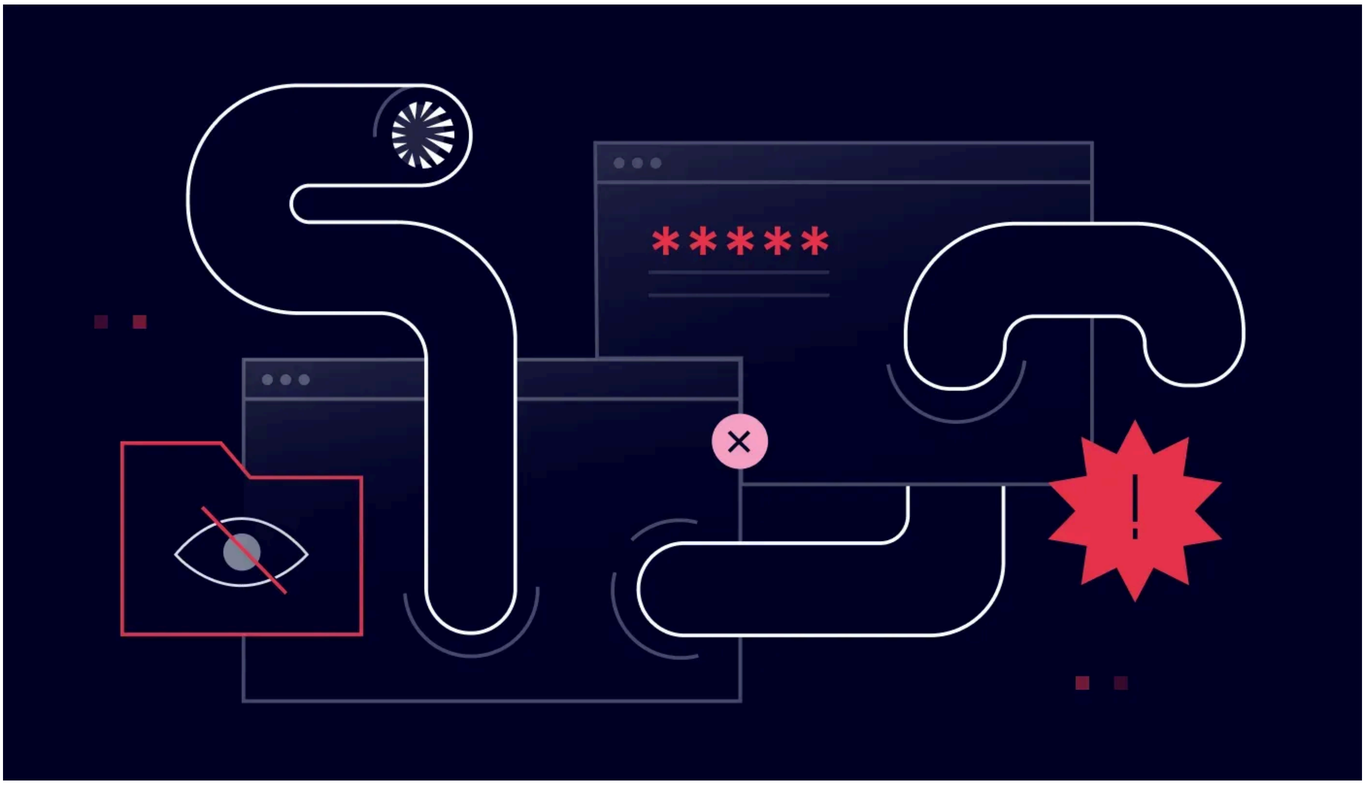
Man-in-the-Middle attacks



A Man-in-the-Middle (MITM) attacks **intercept communication between two parties, altering or stealing sensitive data**. They often exploit social engineering to gain access, which can lead to significant data breaches as the attacker positions themselves between the sender and the recipient, becoming a "middleman" in the process.

This type is different from other phishing attacks because the source is entirely genuine. It's just that it's been altered to serve the hacker's goals. An obvious example would be attacking an organization's financial department and changing the bank transfer code. As neither party notices anything unusual, this cyber attack type is tough to detect and is usually discovered after the attack.

Related articles

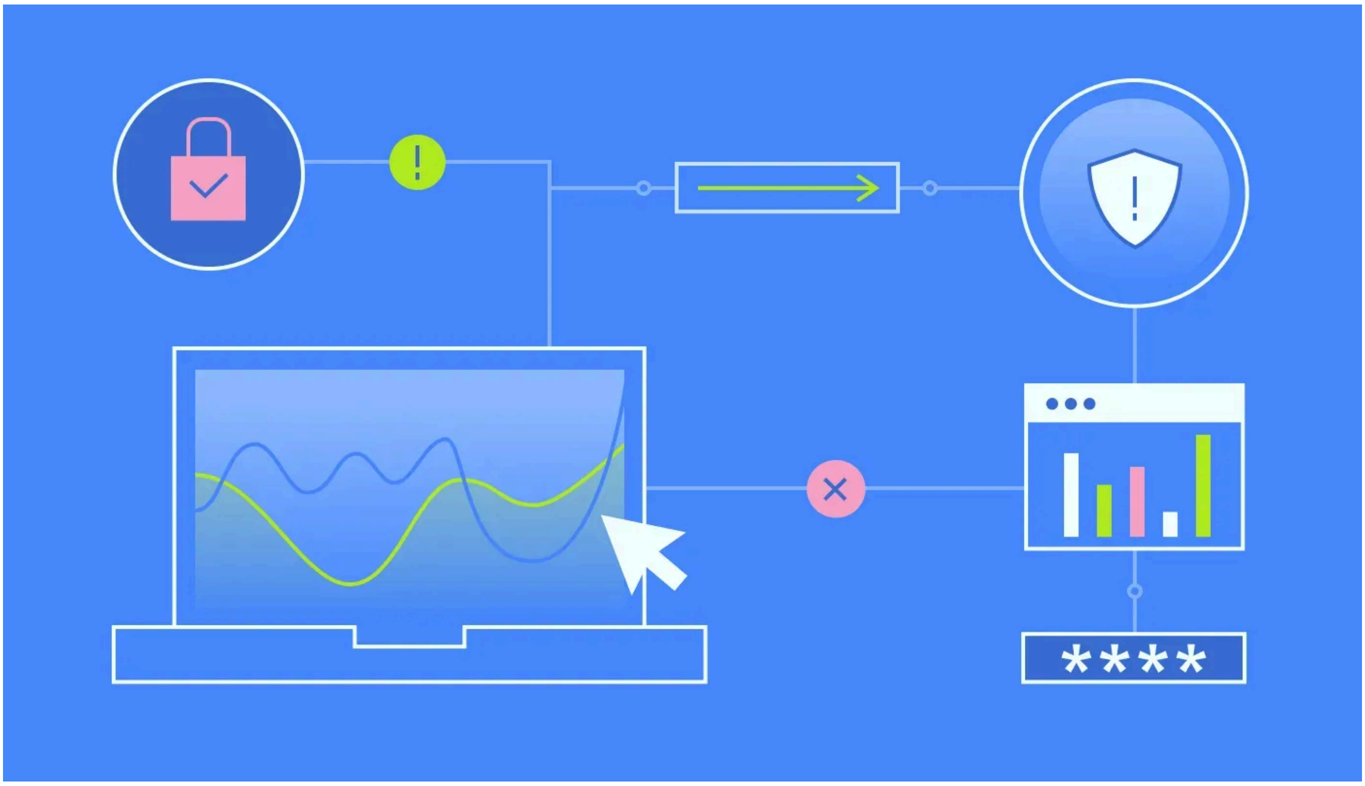


NETWORK SECURITY

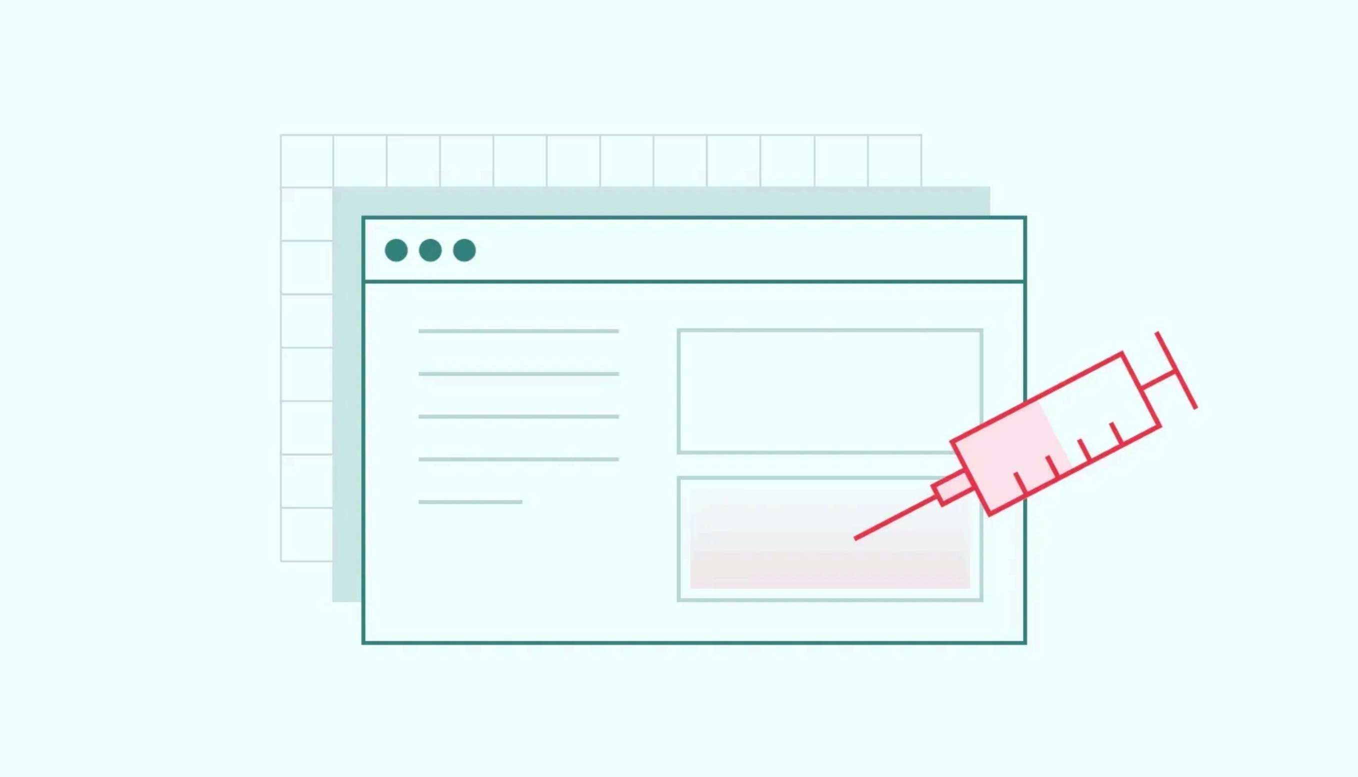
How to prevent phishing attacks: best strategies

Anastasiya Novikava

Apr 10, 2024 10 min read



SQL injection

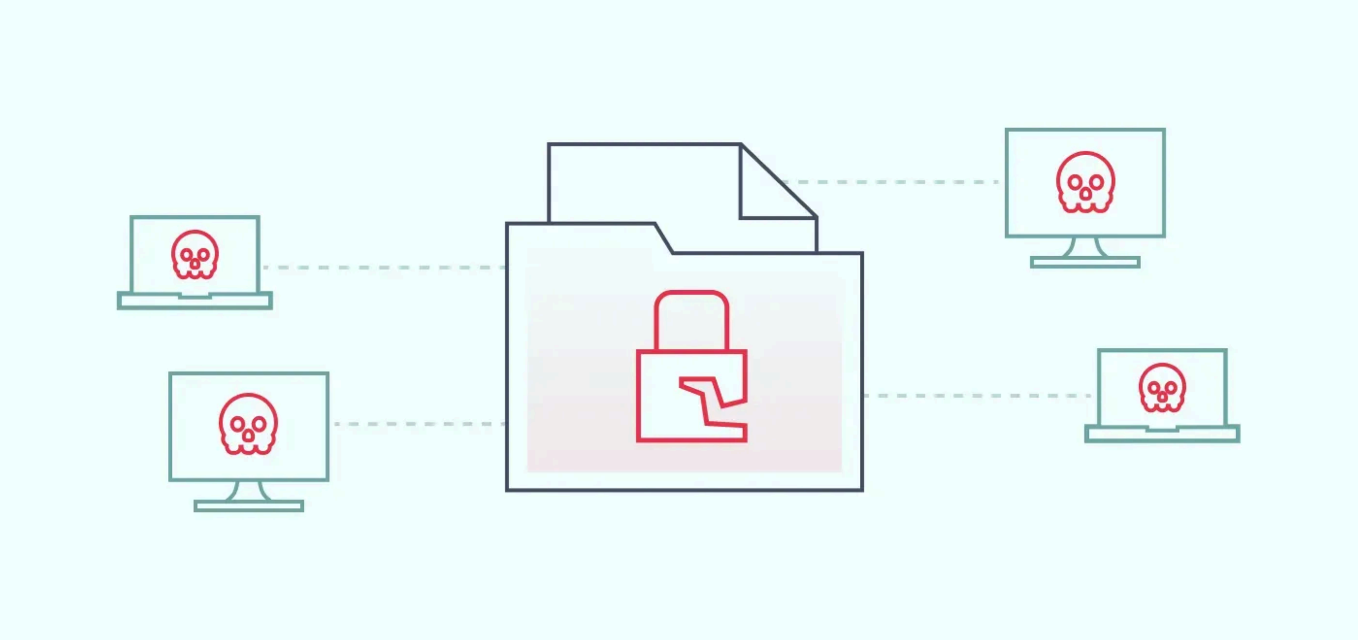


SQL (Structured Query Language) injection exploits vulnerable input fields in web applications, allowing attackers to **manipulate databases to steal, modify, or delete data**. As many applications and websites dynamically construct SQL queries by combining the user-supplied input and the query string, this provides a window of opportunity for hackers.

The attacker identifies a vulnerable input field in a web application that accepts user input, like a login form, search box, or any other input field. Then, a crafted input with SQL code needs to be submitted as part of the user input. If the application takes input as a SQL query without validation, it can be executed by the application's database engine. It interprets the injected SQL query as part of the malicious code infiltrating the database.

SQL injection allows hackers to perform many unauthorized actions like bypassing authentication, retrieving sensitive data, modifying or deleting database records, or executing arbitrary commands on the underlying system.

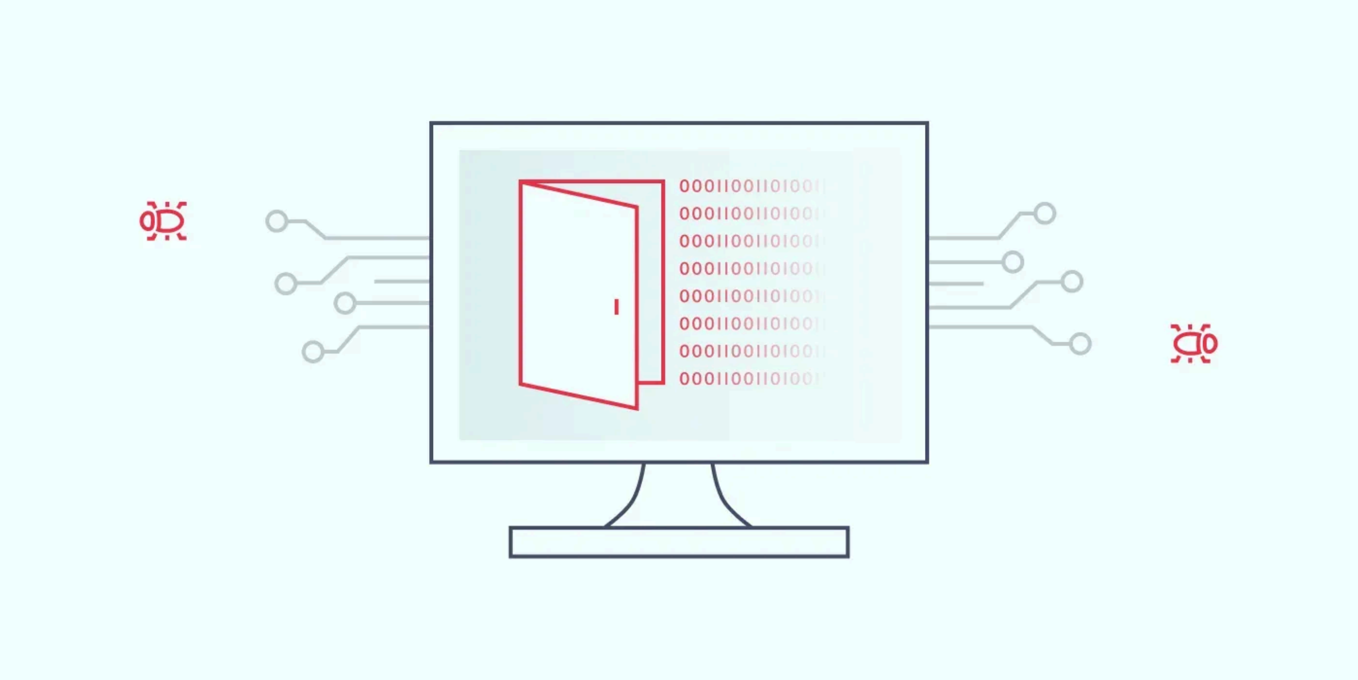
DDoS attacks



A Distributed Denial of Service (DDoS) attack is **a malicious attempt to disrupt the normal functioning of a computer network, service, or website by overwhelming it with a flood of illegitimate traffic**. In a DDoS attack, multiple compromised devices or systems are used to generate a massive volume of requests or data packets toward a target, overwhelming its resources and making it unavailable to legitimate users.

These attacks can be launched from anywhere, making them highly challenging to mitigate. Furthermore, attackers often employ tactics like IP address spoofing or multiple attack vectors simultaneously, making it more challenging to identify and block malicious traffic.

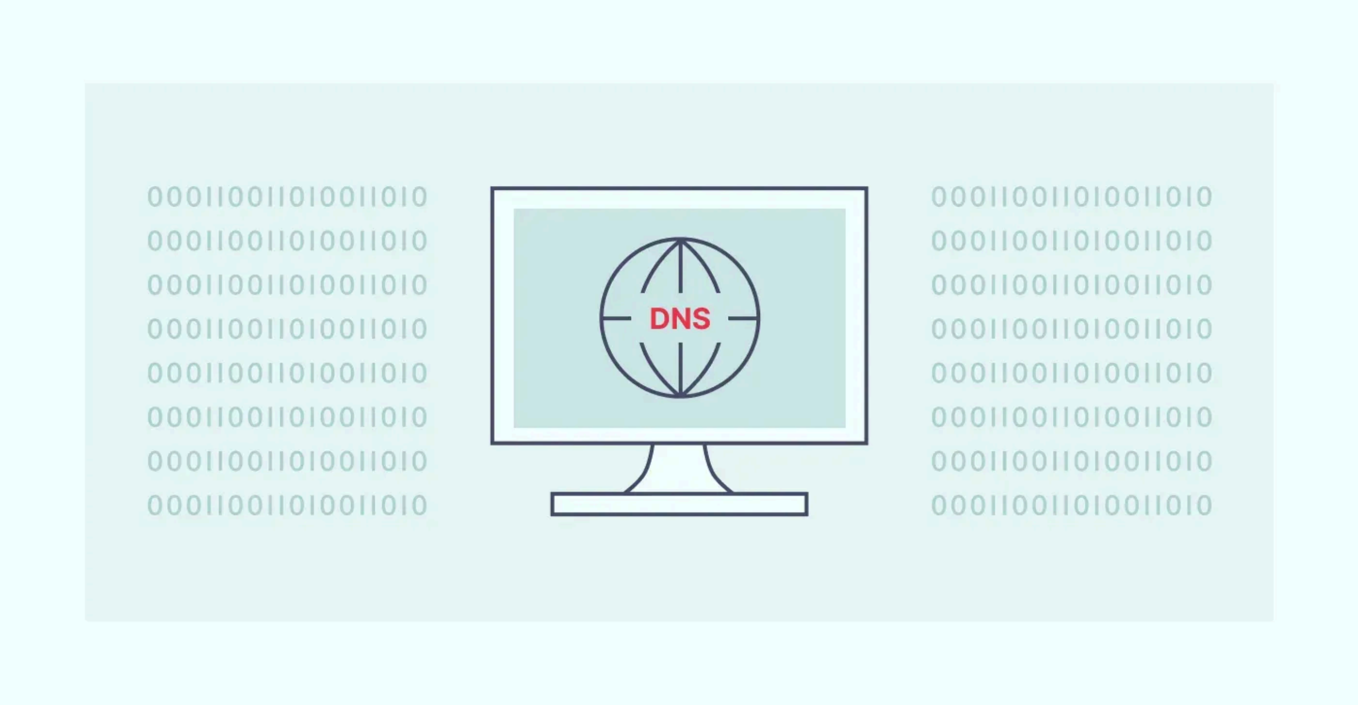
Zero-day exploits



Zero-day exploits refer to **unknown security vulnerabilities or weaknesses in software, operating systems, or applications**. They have no official patches because developers had zero days to address them before they were exploited.

These exploits are highly sought after by both cybercriminals and security researchers because they provide a significant advantage to the attacker. Zero-day exploits are dangerous because there are no available defenses or countermeasures.

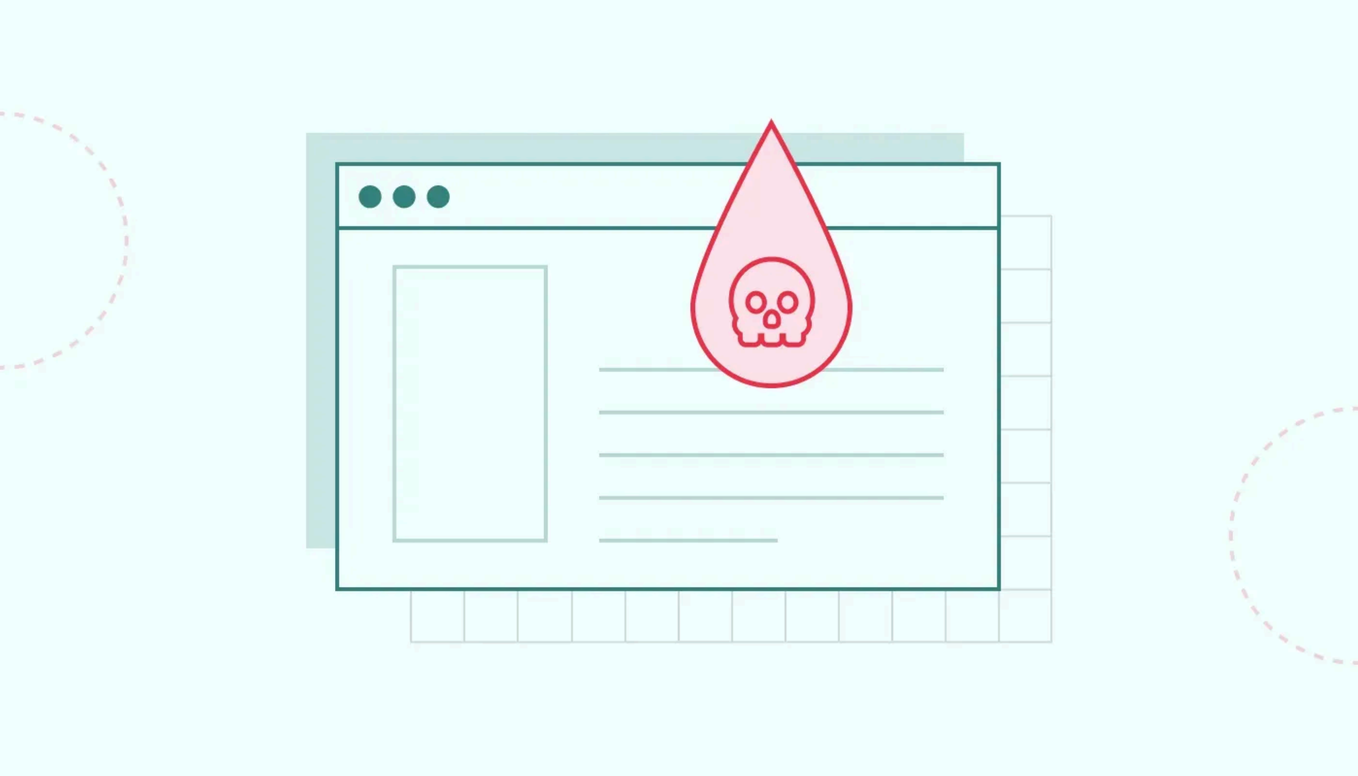
DNS tunneling



DNS tunneling is **a technique to bypass security measures and exfiltrate data from a network**. The attacker exploits the DNS protocol to establish a covert communications channel between a compromised machine within a network and an external server controlled by the attacker. It allows them to send and receive unauthorized data through DNS queries and responses.

DNS tunneling poses a significant security risk because it leverages a widely used and trusted protocol to bypass firewalls and other security measures that typically monitor and restrict data traffic. By hiding within DNS traffic, attackers can exfiltrate data without arousing suspicion.

XSS attacks



Cross-Site Scripting (XSS) attacks **inject malicious scripts into websites that users trust**, aiming to steal sensitive data. XSS attacks typically target web applications that allow user-generated content, such as online forums, comment sections, or input fields.

The attacker finds a vulnerable website and identifies the input field for submitting comments, search queries, or any other user input form. A malicious payload is then crafted using scripts or code, often written in JavaScript. Unaware of malicious intent, the website accepts and stores or displays the input. When users interact with the compromised web page, the website serves the malicious payload to their browser. It leads to malicious code execution in the victim's browser.

Common cyber-attacks on SMBs

Cybercriminals often target small businesses because they typically have less secure networks and less sophisticated cybersecurity measures than large corporations. At the same time, they still have enough sensitive information to be attractive targets.

Phishing is the most popular attack against SMBs because it requires the least preparation time. All a hacker needs is a convincing email message, adjusting the formatting, and sometimes spoofing an email's domain address while dodging spam filters. Then all that's left to do is wait for the victim to click the link.

Malware involves all varieties of malicious software, there are countless ways and methods of how an SMB could come into contact with it. Malware can range from ransomware that encrypts files and demands a ransom to release them to spyware that collects and sends sensitive data to the attacker.

DDoS and other DoS attacks due to their disruptive nature often target organizations and businesses. Business services can be completely shut down, making it impossible for legitimate users to access the system. Small businesses can become targets of such attacks as digital vandalism or as a distraction for another type of attack.

Staying ahead of cyber threats with NordLayer

Advanced technologies like artificial intelligence are increasingly used to predict and mitigate potential attacks, including phishing, ransomware, and malware attacks. Organizations should implement multi-factor authentication, robust firewalls, and regular security awareness training to protect themselves against social engineering and other attack vectors. Advanced tools like NordLayer's Threat Blocker and Zero Trust Network Access (ZTNA) provide additional layers of defense to prevent today's most common network security threats:

- Secure Remote Access: Safeguard remote workforces with encrypted connections, ensuring employees can access critical resources securely from anywhere

- Cloud Firewall: Control and monitor incoming and outgoing traffic with advanced filtering, blocking malicious activity before it reaches your network
- Threat Blocker: Automatically identify and block access to malicious websites, phishing links, or suspicious content, reducing the risk of human error
- Zero Trust Network Access (ZTNA): Adopt a "never trust, always verify" approach to restrict access based on identity and context, minimizing exposure to insider and outsider threats
- Centralized management: Easily manage users, devices, and permissions through an intuitive dashboard, helping you maintain compliance and visibility across your network

While no single solution eliminates every threat, NordLayer offers a robust suite of tools that strengthen defenses and enhance incident response. From encrypting sensitive data to implementing granular access controls, these features empower businesses to build resilience against cyber-attacks.

Contact our team to discover the right solutions for your organization.

FAQ

How often do cyber-attacks occur?

Cyber-attacks occur daily, with thousands of incidents reported worldwide. In 2024, the frequency of attacks has increased significantly, with both ransomware attacks and phishing being among the most common methods cybercriminals employ.

What is the most significant cybersecurity incident in 2024?

In February 2024, Change Healthcare, a key healthcare provider in the U.S., was hit by a ransomware attack that crippled operations across many hospitals. The attackers demanded $22 million to restore access to systems critical for operations like claims processing and prescription drug management. Change Healthcare decided to pay the ransom to minimize disruption to patient care.

What are the top 3 most common cyber-attacks in 2024?

The top cybersecurity threats in 2024 are phishing, ransomware, and malware. Phishing remains prevalent due to its effectiveness in deceiving users, while ransomware attacks have surged, targeting various sectors for financial gain.

Agnė Srėbaliūtė

Senior Creative Copywriter

Agne is a writer with over 15 years of experience in PR, SEO, and creative writing. With a love for playing with words and meanings, she creates unique content. Introverted and often lost in thought, Agne balances her passion for the tech world with hiking adventures across various countries. She appreciates the IT field for its endless learning opportunities.

Share this post

f 𝕏 in 🔗

Related Articles