**Vector (malware)**

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Vector_(malware)#mw-head) [Jump to search](https://en.wikipedia.org/wiki/Vector_(malware)#searchInput)

|  |  |
| --- | --- |
|  | This article **needs additional citations for** [**verification**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this article](https://en.wikipedia.org/w/index.php?title=Vector_(malware)&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Referencing_for_beginners). Unsourced material may be challenged and removed. *Find sources:* ["Vector" malware](https://www.google.com/search?as_eq=wikipedia&q=%22Vector%22+malware) – [news](https://www.google.com/search?tbm=nws&q=%22Vector%22+malware+-wikipedia) **·** [newspapers](https://www.google.com/search?&q=%22Vector%22+malware+site:news.google.com/newspapers&source=newspapers) **·** [books](https://www.google.com/search?tbs=bks:1&q=%22Vector%22+malware+-wikipedia) **·** [scholar](https://scholar.google.com/scholar?q=%22Vector%22+malware) **·** [JSTOR](https://www.jstor.org/action/doBasicSearch?Query=%22Vector%22+malware&acc=on&wc=on) *(March 2017) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

A **vector** in [computing](https://en.wikipedia.org/wiki/Computing), specifically when talking about malicious code such as [viruses](https://en.wikipedia.org/wiki/Computer_virus) or [worms](https://en.wikipedia.org/wiki/Computer_worm), is the *method* that this code uses to propagate itself or infect a computer. This sense is similar to, and derived from, its [meaning in biology](https://en.wikipedia.org/wiki/Vector_(epidemiology)).

Some common vectors:

* [buffer overflows](https://en.wikipedia.org/wiki/Buffer_overflow) – this is how the [Blaster worm](https://en.wikipedia.org/wiki/Blaster_worm) was able to propagate
* HTML email with [JavaScript](https://en.wikipedia.org/wiki/JavaScript) or other scripting enhancements
* networking protocol flaws

**Web-based malware and vector**

According to Provos et al., a web page is determined malicious "if it causes the automatic installation of software without the user's knowledge or consent". To increase the success rate of the vector (malware), malware is usually camouflaged by layers of code.[[1]](https://en.wikipedia.org/wiki/Vector_(malware)#cite_note-:0-1)

Types of web-based malware include:

1. [Trojan](https://en.wikipedia.org/wiki/Trojan_horse_(computing))
2. [Adware](https://en.wikipedia.org/wiki/Adware)
3. Unknown/Obfuscated: "A binary that has been obfuscated so that we could not determine its functionality."[[1]](https://en.wikipedia.org/wiki/Vector_(malware)#cite_note-:0-1)

In [cybersecurity](https://www.upguard.com/blog/cyber-security), an attack vector is a path or means by which an attacker can gain unauthorized access to a computer or network to deliver a payload or malicious outcome. Attack vectors allow attackers to [exploit](https://www.upguard.com/blog/exploit) system [vulnerabilities](https://www.upguard.com/blog/vulnerability), install different [types of malware](https://www.upguard.com/blog/types-of-malware) and launch [cyber attacks](https://www.upguard.com/blog/cyber-attack).

Attack vectors can also be exploited to gain access to [sensitive data](https://www.upguard.com/blog/sensitive-data), [personally identifiable information (PII)](https://www.upguard.com/blog/personally-identifiable-information-pii) and other sensitive information that would result in a [data breach](https://www.upguard.com/blog/data-breach). And with the average [cost of a data breach](https://www.upguard.com/blog/cost-of-data-breach) at $3.92 million, it pays to think through how to minimize potential attack vectors and [prevent data breaches](https://www.upguard.com/blog/prevent-data-breaches).

[Digital forensics](https://www.upguard.com/blog/digital-forensics) and [IP attribution](https://www.upguard.com/blog/ip-attribution) are only so helpful for cleaning up data breaches, it's much more important to prevent them.

Common attack vectors include malware, viruses, email attachments, web pages, pop-ups, instant messages, text messages and [social engineering](https://www.upguard.com/blog/social-engineering).

The number of [cyber threats](https://www.upguard.com/blog/cyber-threat) is on the rise as cyber criminals look for exploit unpatched vulnerabilities listed on [CVE](https://www.upguard.com/blog/cve) and the [dark web](https://www.upguard.com/blog/dark-web), and no one solution can prevent every attack vector. Cyber criminals are increasingly sophisticated and it is no longer enough to rely on an antivirus as your sole security system.

This is why organizations must employ [defense in depth](https://www.upguard.com/blog/defense-in-depth) to minimize [cybersecurity risk](https://www.upguard.com/blog/cybersecurity-risk).

## Table of contents

1. [What is the difference between an attack vector, attack surface and data breach?](https://www.upguard.com/blog/attack-vector#difference)
2. [Why are attack vectors exploited by attackers?](https://www.upguard.com/blog/attack-vector#why)
3. [How do attackers exploit attack vectors?](https://www.upguard.com/blog/attack-vector#how)
4. [What are the common types of attack vectors?](https://www.upguard.com/blog/attack-vector#common-attack-vectors)
5. [How UpGuard can help you understand your organization's attack surface](https://www.upguard.com/blog/attack-vector#upguard)

## 1. What is the difference between an attack vector, attack surface and data breach?

* **Attack vector:** A method or way an attacker can gain unauthorized access to a network or computer system.
* [**Attack surface**](https://www.upguard.com/blog/attack-surface)**:** The total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.
* **Data breach:** Any security incident where sensitive, protected, or confidential data is accessed or stolen by an unauthorized party.

## 2. Why are attack vectors exploited by attackers?

Cyber criminals can make money from attacking your organization's software systems, such as stealing credit card numbers or online banking credentials. However, there are other more sophisticated ways to monetize their actions that aren't as obvious as stealing money.

Attackers may infect your system with [malware](https://www.upguard.com/blog/malware) that grants remote access to a command and control server. Once they have infected hundreds or even thousands of computers they can establish a botnet, which can be used to send [phishing](https://www.upguard.com/blog/phishing) emails, launch other [cyber attacks](https://www.upguard.com/blog/cyber-attack), steal [sensitive data](https://www.upguard.com/blog/sensitive-data) or mine cryptocurrency.

Another common motivation is to gain access to [personally identifiable information (PII)](https://www.upguard.com/blog/personally-identifiable-information-pii), healthcare information and [biometrics](https://www.upguard.com/blog/biometrics) to commit insurance fraud, credit card fraud or to illegally obtain prescription drugs.

Competitors may employ attackers to perform [corporate espionage](https://www.upguard.com/blog/corporate-espionage) or overload your data centers with a Distributed Denial of Service (DDoS) attack to cause downtime, harm sales and cause customers to leave your business.

Money is not the only motivator. Attackers may want to leak information to the public, embarrass your organization, be motivated by political ideologies, or be performing cyber warfare on behalf of a nation state like the United States or China.

## 3. How do attackers exploit attack vectors?

There are many ways to expose, alter, disable, destroy, steal or gain unauthorized access to computer systems, infrastructure, networks, operating systems and IoT devices.

In general, attack vectors can be split into passive or active attacks:

* **Passive:** attempts to gain access or make use of information from the system but does not affect system resources, such as [typosquatting](https://www.upguard.com/blog/typosquatting), [phishing](https://www.upguard.com/blog/phishing) and other [social engineering](https://www.upguard.com/blog/social-engineering) based attacks.
* **Active:** attempts to alter a system or affect its operation such as [malware](https://www.upguard.com/blog/malware), exploiting unpatched [vulnerabilities](https://www.upguard.com/blog/vulnerability), [email spoofing](https://www.upguard.com/blog/email-spoofing), [man-in-the-middle attacks](https://www.upguard.com/blog/man-in-the-middle-attack), [domain hijacking](https://www.upguard.com/blog/domain-hijacking) and [ransomware](https://www.upguard.com/blog/ransomware).

That said, most attack vectors share similarities:

* Attacker identifies a potential target.
* Attacker gathers information about the target using [social engineering](https://www.upguard.com/blog/social-engineering), [malware](https://www.upguard.com/blog/malware), [phishing](https://www.upguard.com/blog/phishing), [OPSEC](https://www.upguard.com/blog/opsec) and automated [vulnerability](https://www.upguard.com/blog/vulnerability) scanning.
* Attackers use the information to identify possible attack vectors and create or use tools to exploit them.
* Attackers gain unauthorized access to the system and steal [sensitive data](https://www.upguard.com/blog/sensitive-data) or install malicious code.
* Attackers monitor the computer or network, steal information or use computing resources.

One often overlooked attack vector are your [third and fourth-party vendors](https://www.upguard.com/blog/third-party-vendor) and service providers. It doesn't matter how sophisticated your internal [network security](https://www.upguard.com/blog/network-security) and [information security](https://www.upguard.com/blog/information-security) is, if vendors have access to [sensitive data](https://www.upguard.com/blog/sensitive-data) they are as much a risk to your organization.

This is why it is important to measure and mitigate [third-party risk](https://www.upguard.com/articles/five-things-to-know-about-third-party-risk) and [fourth-party risk](https://www.upguard.com/blog/what-is-fourth-party-risk). This means it needs to be part of your [information security policy](https://www.upguard.com/blog/information-security-policy) and [information risk management](https://www.upguard.com/blog/information-risk-management) program.

Consider investing in threat intelligence tools that help [automate vendor risk management](https://www.upguard.com/blog/automate-vendor-risk-management) and [automatically monitor your vendor's security posture and notify you if it worsens](https://www.upguard.com/product/vendorrisk).

Every organization now needs a [third-party risk management framework](https://www.upguard.com/blog/third-party-risk-management-framework), [vendor management policy](https://www.upguard.com/blog/vendor-management-policy) and [vendor risk management](https://www.upguard.com/blog/vendor-risk-management) program.

Before considering a new vendor perform a [cybersecurity risk assessment](https://www.upguard.com/blog/cyber-security-risk-assessment) to understand what attack vectors you could be introducing to your organization by using them and ask about  their [SOC 2 compliance.](https://www.upguard.com/blog/soc-2)

## 4. What are the common types of attack vectors?

* **Compromised credentials:**Usernames and passwords are still the most common type of access credential and continue to be exposed in [data leaks](https://www.upguard.com/blog/data-leak), [phishing scams](https://www.upguard.com/blog/phishing) and by [malware](https://www.upguard.com/blog/malware). When lost, stolen or exposed, credentials give attackers unfettered access. This is why organizations are now investing in tools to continuously monitor for [data exposures and leaked credentials](https://www.upguard.com/product/breachsight). Password managers, two-factor authentication and [biometrics](https://www.upguard.com/blog/biometrics) can reduce the risk of leak credentials resulting in a security incident too.
* **Weak credentials:**Weak passwords and reused passwords mean one data breach can result in many more. Teach your organization [how to create a secure password](https://www.upguard.com/blog/the-password-security-checklist), invest in a password manager or a single sign-on tool, and educate staff on their benefits.
* **Malicious insiders:**Disgruntled employees can expose private information or provide information about company specific [vulnerabilities](https://www.upguard.com/blog/vulnerability).
* **Missing or poor encryption:**Common [encryption](https://www.upguard.com/blog/encryption) methods like [SSL certificates](https://www.upguard.com/blog/ssl-certificate) and [DNSSEC](https://www.upguard.com/blog/dnssec) can prevent [man-in-the-middle attacks](https://www.upguard.com/blog/man-in-the-middle-attack) and protect the confidentiality of data being transmitted. Missing or poor encryption for data at rest can mean that sensitive data or credentials are exposed in the event of a [data breach](https://www.upguard.com/blog/data-breach) or [data leak](https://www.upguard.com/blog/data-leak).
* **Misconfiguration:**Misconfiguration of cloud services, like Google Cloud Platform,  Microsoft Azure or AWS, or using default credentials can lead to data breaches and data leaks, [check your S3 permissions or someone else will](https://www.upguard.com/blog/check-your-amazon-s3-permissions-someone-will). Automate configuration management where possible to prevent configuration drift.
* **Ransomware:**[Ransomware](https://www.upguard.com/blog/ransomware) is a form of extortion where data is deleted or encrypted unless a ransom is paid, such as [WannaCry](https://www.upguard.com/blog/wannacry). Minimize the impact of ransomware attacks by keeping your systems patched and backing up important data.
* **Phishing:**[Phishing](https://www.upguard.com/blog/phishing) is a [social engineering](https://www.upguard.com/blog/social-engineering) technique where the target is contacted by email, telephone or text message by someone who is posing to be a legitimate colleague or institution to trick them into providing [sensitive data](https://www.upguard.com/blog/sensitive-data), credentials or [personally identifiable information (PII)](https://www.upguard.com/blog/personally-identifiable-information-pii). To minimize phishing, educate your staff on [the importance of cybersecurity](https://www.upguard.com/blog/cybersecurity-important) and prevent [email spoofing](https://www.upguard.com/blog/email-spoofing) and [typosquatting](https://www.upguard.com/blog/typosquatting).
* **Vulnerabilities:**New vulnerabilities are added to [CVE](https://www.upguard.com/blog/cve) every day and [zero-day vulnerabilities](https://www.upguard.com/blog/zero-day) are found just as often. If a developer has not released a patch for a zero-day vulnerability before an attack can exploit it, it can be hard to prevent.
* **Brute force:**[Brute force attacks](https://www.upguard.com/blog/brute-force-attack) are based on trial and error. Attackers may continuously try to gain access to your organization until one attack works. This could be by attacking weak passwords or encryption, phishing emails or sending infected email attachments containing a [type of malware](https://www.upguard.com/blog/types-of-malware). [Read our full post on brute force attacks](https://www.upguard.com/blog/brute-force-attack).
* **Distributed Denial of Service (DDoS):**DDoS are [cyber attacks](https://www.upguard.com/blog/cyber-attack) against networked resources like data centers, servers or websites and can limit the availability of a computer system. The attacker floods the network resource with messages which cause it to slow down or even crash, making it inaccessible to users. Potential mitigations include CDNs and proxies.
* **SQL injections:**SQL stands for structured query language, a programming language used to communicate with databases. Many of the servers that store [sensitive data](https://www.upguard.com/blog/sensitive-data) use SQL to manage the data in their database. An SQL injection uses malicious SQL to get the server to expose information it otherwise wouldn't. This is a huge [cyber risk](https://www.upguard.com/blog/cyber-risk) if the database stores customer information, credit card numbers, credentials or other [personally identifiable information (PII)](https://www.upguard.com/blog/personally-identifiable-information-pii).
* **Trojans:**Trojan horses are malware that misleads users by pretending to be a legitimate program and are often spread via infected email attachments or fake software.
* **Cross-site scripting (XSS):**[XSS attacks](https://www.upguard.com/blog/cross-site-scripting-xss) involve injecting malicious code into a website but the website itself is not being attacked, rather it aims to impact the website's visitors. A common way attackers can deploy cross-site scripting attacks is by injecting malicious code into a comment e.g. embed a link to malicious JavaScript in a blog post's comment section.
* **Session hijacking:**When you log into a service, it generally provides your computer with a session key or cookie so you don't need to log in again. This cookie can be hijacked by an attacker who uses it to gain access to sensitive information.
* **Man-in-the-middle attacks:**Public Wi-Fi networks can be exploited to perform [man-in-the-middle attacks](https://www.upguard.com/blog/man-in-the-middle-attack) and intercept traffic that was supposed to go elsewhere, such as when you log into a secure system.
* **Third and fourth-party vendors:**The rise in outsourcing means that your vendors pose a huge [cybersecurity risk](https://www.upguard.com/blog/cybersecurity-risk) to your customers data and your proprietary data. Some of the [biggest data breaches](https://www.upguard.com/blog/biggest-data-breaches) were caused by third-parties.