Cybersecurity

What is an Attack Vector? 16 Common Attack Vectors in 2022

Abi Tyas Tunggal
updated Jun 17, 2022

In cybersecurity, an attack vector is a method of achieving unauthorized network access to launch a cyber attack.

Attack vectors allow cybercriminals to exploit system vulnerabilities to gain access to sensitive data, personally identifiable information (PII), and other valuable information accessible after a data breach.

With the average cost of a data breach at $4.24 million, it's imperative to think through how to minimize potential attack vectors and prevent data breaches.

Digital forensics and IP attribution are only so helpful for cleaning up data breaches, it's much more important to prevent them.

messages, and social engineering.

The number of cyber threats is on the rise as cybercriminals look for exploit unpatched vulnerabilities listed on CVE and the dark web, and no one solution can prevent every attack vector. Cybercriminals are increasingly sophisticated and it is no longer enough to rely on antivirus software as primary security system.

This is why organizations must employ defense in depth to minimize cybersecurity risk.

Contents

Author

Abi Tyas Tunggal

Reviewed by

Kaushik Sen

What is the Difference Between an Attack Vector, Attack Surface and Data Breach?

An attack vector is a method of gaining unauthorized access to a network or computer system.

An attack surface is the total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.

A Data breach is any security incident where sensitive, protected, or confidential data is accessed or stolen by an unauthorized party.

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 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 emails, launch other cyber attacks, steal sensitive data or mine cryptocurrency.

Another common motivation is to gain access to personally identifiable information (PII), healthcare information and biometrics to commit insurance fraud, credit card fraud or to illegally obtain prescription drugs.

Competitors may employ attackers to perform 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.

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 Attack Vector Exploits

Passive attack vector exploits are attempts to gain access or make use of information from the system but does not affect system resources, such as typosquatting, phishing and other social engineering based attacks.

Active Attack Vector Exploits

Active attack vector exploits are attempts to alter a system or affect its operation such as malware, exploiting unpatched vulnerabilities, email spoofing, man-in-the-middle attacks, domain hijacking and ransomware.

That said, most attack vectors share similarities:

- Attacker identifies a potential target.
- Attacker gathers information about the target using social engineering, malware, phishing, OPSEC and automated 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 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 and service providers. It doesn't matter how sophisticated your internal network security and information security is, if vendors have access to sensitive data they are as much a risk to your organization.

This is why it is important to measure and mitigate third-party risk and fourth-party risk. This means it needs to be part of your information security policy and information risk management program.

Consider investing in threat intelligence tools that help automate vendor risk management and automatically monitor your vendor's security posture and notify you if it worsens.

Every organization now needs a third-party risk management framework, vendor management policy and vendor risk management program.

Before considering a new vendor perform a cybersecurity risk assessment to understand what attack vectors you could be introducing to your organization by using them and ask about their SOC 2 compliance.

What are the Common Types of Attack Vectors?

1. Compromised Credentials

Usernames and passwords are still the most common type of access credential and continue to be exposed in data leaks, phishing scams and by 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. Password managers, two-factor authentication and biometrics can reduce the risk of leak credentials resulting in a security incident too.

2. 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, invest in a password manager or a single sign-on tool, and educate staff on their benefits.

3. Malicious Insiders

Disgruntled employees can expose private information or provide information about company specific vulnerabilities.

4. Missing or Poor Encryption

Common encryption methods like SSL certificates and DNSSEC can prevent man-in-the-middle attacks 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 or data leak.

5. 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. Automate configuration management where possible to prevent configuration drift.

6. Ransomware

Ransomware is a form of extortion where data is deleted or encrypted unless a ransom is paid, such as WannaCry. Minimize the impact of ransomware attacks by maintaining a defense plan, including keeping your systems patched and backing up important data.

7. Phishing

Phishing is a 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, credentials or personally identifiable information (PII). To minimize phishing, educate your staff on the importance of cybersecurity and prevent email spoofing and typosquatting.

8. Vulnerabilities

New vulnerabilities are added to CVE every day and zero-day vulnerabilities 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.

9. Brute Force

Brute force attacks 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. Read our full post on brute force attacks.

10. Distributed Denial of Service (DDoS)

DDoS are cyber attacks 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.

11. SQL Injections

SQL stands for structured query language, a programming language used to communicate with databases. Many of the servers that store 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 if the database stores customer information, credit card numbers, credentials or other personally identifiable information (PII).

12. 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.

13. Cross-Site Scripting (XSS)

XSS attacks 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.

14. 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.

15. Man-in-the-Middle Attacks

Public Wi-Fi networks can be exploited to perform man-in-the-middle attacks and intercept traffic that was supposed to go elsewhere, such as when you log into a secure system.

16. Third and Fourth-Party Vendors

The rise in outsourcing means that your vendors pose a huge cybersecurity risk to your customer's data and your proprietary data. Some of the biggest data breaches were caused by third parties.

FAQ About Attack Vectors

What is an attack vector?

An attack vector is a potential pathway into sensitive resources that could facilitate a data breach if exploited.

Why are attack vectors exploited in cyberattacks?

The primary motivator of cyberattacks is monetary gain, but this isn't always the case. Some cyberattacks are motivated by public humiliation. Many cyber incidents aim to eliminate competitors.

How can you locate attack vectors?

Attack vectors are linked to security vulnerabilities in your network, so by using an attack surface monitoring solution, you'll be able to locate attack vectors throughout your threat landscape.

What are the most common attack vectors?

The most common attack vectors are:

- Phishing emails
- Malware
- Unpatched vendor software

- Ransomware
- Insider threats
- Weak credentials
- Third-party vendors
- Poor encryption
- Poor system configuration

Address All of Your Attack Vectors With UpGuard

At UpGuard, we can protect your business from data breaches, identify all of your data leaks, and help you continuously monitor the security posture of all your vendors.

UpGuard also supports compliance across a myriad of security frameworks, including the new requirements set by Biden's Cybersecurity Executive Order.

CLICK HERE to get your FREE security rating now!

Tags: Cybersecurity Attack Surface Management

See UpGuard In Action

Book a free, personalized onboarding call with one of our cybersecurity experts.

Contact sales | Free demo

Related posts

Learn more about the latest issues in cybersecurity.

The Top Cybersecurity Websites and Blogs of 2022

The Top Cybersecurity Websites and Blogs of 2022

This is a complete guide to the best cybersecurity an...

Abi Tyas Tunggal
June 10, 2022

14 Cybersecurity Metrics + KPIs You Must Track in 2022

14 Cybersecurity Metrics + KPIs You Must Track in 2022

Cybersecurity metrics and key performance indicator...

Abi Tyas Tunggal
June 10, 2022

What are Security Ratings?

What are Security Ratings?

This is a complete guide to security ratings and...

Abi Tyas Tunggal
May 11, 2022

Why is Cybersecurity Important?

If your business isn't concerned about...

Abi Tyas Tunggal
June 26, 2022

What is Typosquatting (and How to Prevent It)

Learn about the dangers of typosquatting and what...

Abi Tyas Tunggal
June 26, 2022

What is a Cyber Threat?

What is a Cyber Threat?

A cyber threat (or cybersecurity threat) is...

Abi Tyas Tunggal
June 26, 2022

View all blog posts >

Sign up to our newsletter

Get the latest curated cybersecurity news, breaches, events and updates in your inbox every week.

Email address*

Subscribe

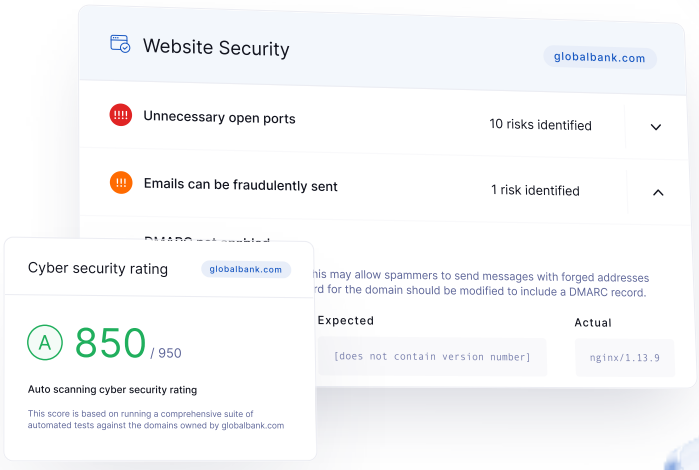
Free instant security score

How secure is your organization?

Request a free cybersecurity report to discover key risks on your website, email, network, and brand.

- Instant insights you can act on immediately
- Hundreds of risk factors including email security, SSL, DNS health, open ports and common vulnerabilities

Free score >



UpGuard

UpGuard is a complete third-party risk and attack surface management platform. Our security ratings engine monitors millions of companies every day.

122 Ratings Submit a review As of 28 Jun 2022

Products
- Guard Vendor Risk
- UpGuard BreachSight

Compare
- BitSight
- SecurityScorecard

Solutions
- Financial Services
- Technology

Company
- About us
- Careers We're hiring!

Insights
- Events Register!
- Breaches