

Drive by Download Attack Definition

Drive by download attacks specifically refer to malicious programs that install to your devices — without your consent. This also includes unintentional downloads of any files or bundled software onto a computer device.

Masked in all corners of the web, these attacks cause even perfectly legitimate sites to spread this threat.

variantsHere are the two main variants of Drive by Download attacks:

- ✓ 1. Non-malicious potentially unwanted programs or applications (PUPs/PUAs).
- ✓ 2. Malware-loaded attacks.

While the former is clean and safe, it may be adware at its worst. Cybersecurity experts use the latter as their drive by download definition.

What is a Drive by Download Attack?

A drive-by download attack refers to the unintentional download of malicious code to your computer or mobile device that leaves you open to a cyberattack. You don't have to click on anything, press download, or open a malicious email attachment to become infected.

A drive-by download can take advantage of an app, operating system, or web browser that contains security flaws due to unsuccessful updates or lack of updates. Unlike many other types of cyberattack, a drive-by doesn't rely on the user to do anything to actively enable the attack.

Effect

Drive by downloads are designed to breach your device for one or more of the following:

1. Hijack your device — to build a botnet, infect other devices, or breach yours further.
2. Spy on your activity — to steal your online credentials, financial info, or identity.
3. Ruin data or disable your device — to simply cause trouble or personally harm you.

Without proper security software or fixes for your vulnerabilities, you could become a victim of a drive by download attack.

How Do Drive by Download Attacks Work?

If you've ever asked yourself, "what is a drive by download attack?" you're more aware than most. Since they infiltrate so quietly even on "safe sites," most people have no clue how they got infected.

There are two main ways malicious drive by downloads get into your devices:

Ways

1. Authorized without knowing full implications: You take an action leading to infection, such as clicking a link on a deceptive fake security alert or downloading a Trojan.
2. Fully unauthorized without any notification: You visit a site and get infected without any prompts or further action.
These downloads can be anywhere, even legitimate sites.

Knowing exactly what is drive by download is as important as knowing how to spot bait for an attack. Let's unpack each one of these methods to help you see possible red flags.

Authorized Downloads with Hidden Payloads

Authorized drive by downloads are streamlined and may even be spotted before the attack:

- Hacker creates a vector for malware delivery — online message, ads, legitimate program downloads.
- You interact with the vector — clicking a deceptive link, downloading software, etc.
- Malware installs on your device — by failing to opt-out of extra software or arriving at a malware-infested site.
- Hacker successfully enters your device — malware takes unwanted control of your data.

Software or websites may seem innocuous, but they are corrupted by malware. In fact, one of the greatest dangers is the ease of attracting visitors to sites or apps that seem innocent.

Cause

For example, you might get a link emailed to you or a post on your social media feed. It is masked to look as though it was sent from sources you trust. This social engineering tactic is used to entice you to click and open. Once the website is open, the drive-by download installs itself on your computer or mobile device. This tactic is used to entice you to click and open. Once the website is open, the drive-by download installs itself on your computer or mobile device.

Bundleware is a popular “authorized” method, using secondary programs attached to your actual desired program download. Sometimes called barnacles, these potentially unwanted programs/applications (PUPs/PUAs) can conceal malware or be malware themselves. You’ll find this software usually as an opt-out choice when downloading free software or shareware.

Phishing can also be used to bait you into a drive-by download. Popups or fraudulent online messages pose as organizations you know and trust. You might be seeing a fake security breach notification from your web browser, or a fake data breach email from your bank. These are meant to scare you into clicking a link or downloading an attachment — and getting infected.

Unauthorized Downloads Without Your Knowledge

Chp
An unauthorized drive by download works in a simple way despite having multiple phases:

1. Hacker compromises a web page — plugging a malicious component into a security flaw.
2. You trigger the component — visiting the page and it finds your device's security gaps.
3. The component downloads malware to your device — via your exploited security.
4. Malware does its job — letting the hacker disrupt, control, or steal from your device.

As noted above, unauthorized malicious code is distributed directly by compromised websites. However, the code is placed there by hackers. Their methods rely on natural flaws of digital technology, as well as unsafe security practices.

Exploit kits are the software used to compromise vulnerable web servers and your devices. These kits identify software vulnerabilities on machines and web browsers to determine which systems are easy to obtain. Exploit kits often use small pieces of code designed to slip past simple defenses and go largely unnoticed. The code is kept simple to focus on one job: to contact another computer to introduce the rest of the code it needs to access a mobile device or computer.

Security vulnerabilities discovered by exploit kits are unavoidable in the digital age. No software or hardware can ever be made perfect. Just like a building can be infiltrated with careful study and planning, so too can any software, network, or other digital infrastructure. Vulnerabilities come in a few common forms:

- Zero-day exploits: Security flaws without any known fixes or patches.

- Known exploits: Security issues that have known-but-uninstalled fixes.

Zero-day exploits are hard to avoid, but known issues are manipulated purely due to poor cybersecurity practices. If endpoint users and web admins fail to update all their software in a timely fashion, they will delay vital security updates as well — and this is what hackers rely on.

Drive by downloads are by far one of the harder threats to prevent. Without proper attention to detail and strong security at all touchpoints, web activity becomes far more hazardous.

How to Avoid Drive by Download Attacks

As with many aspects of cyber safety, the best defense is caution. You should never take your security for granted. Here at Kaspersky, we've compiled some of the best guidelines on how you can avoid downloading malicious code.

How Website Owners Can Prevent Drive by Downloads

As a website owner, you are the first line of defense between hackers that target your users. To give yourself and your users peace-of-mind, strengthen your infrastructure with these tips:

1. Keep all website components up to date. This includes any themes, addons, plugins, or any other infrastructure. Each update likely has new security fixes to keep hackers out.
2. Remove any outdated or unsupported components of your website. Without regular security patches, old software is perfect for frauds to study and exploit.
3. Use strong passwords and usernames for your admin accounts. Brute force attacks give hackers an almost instant break-in for default passwords, or weak ones like

“password1234.” Use a password generator alongside a password manager to stay safe.

4. Install protective web security software into your site. Monitoring software will help keep watch for any malicious changes to your site’s backend code.
5. Consider how your advertisement use might affect users. Advertisements are a popular vector for drive by downloads. Be sure your users aren’t getting recommended suspect advertisements.

7 Tips for Endpoint Users

As a user, you’ll have to rely more on the various security features offered in your software. You can follow these tips to prepare yourself and your software against a drive by download attack:

1. Only use your computer’s admin account for program installations. Admin privileges are necessary for drive by downloads to install without your consent. Since this setting comes default on your main account, use a secondary non-admin account for daily use.
2. Keep your web browser and operating system up to date. New patches help seal gaps in their defenses where drive-by-download code could burrow in. Do not wait or delay — install these updates as soon as they release.
3. Be wary of keeping too many unnecessary programs and apps. The more plug-ins you have on your device, the more susceptible you are to infection. Only keep the software you trust and use often. Also, remove any older apps that no longer receive updates.
4. Use an internet security software solution on all your devices. Products like Kaspersky Security Cloud automatically keep your malware definitions up-to-

date to spot the latest threats. They also can scan websites proactively to block known compromised sites.

5. Always avoid websites that may contain malicious code. Sites that offer file-sharing or mature content are common points of infection. Only visit mainstream sites you normally use or at least well-established sites to improve your chances of staying clean.
6. Carefully read and examine security popups on the web before clicking. Scammers use deceptive popup ads on desktop and mobile browsers that look like legitimate alerts. To avoid being linked to an attack site, watch for typos, odd grammar, and grainy images.
7. Use an ad-blocker. Drive-by download attacks often use online ads to upload infections. Using an ad blocker can help reduce your exposure to this type of attack.



What is a spam attack?

- Spam attacks are defined as an organized and unauthorized use of an app to send thousands of messages to its users.
- These messages are sent by fake or hacked profiles, and often include unreal advertisements and links to which real users are asked to click on.
- Such attacks can have a large and negative impact on the user's enjoyment of the app.

What can I do to help?

If you ever receive an advertisement from other users promoting websites or stating that you won a prize, do NOT click the links. These attacks feed on the number of clicks these links have: the more clicks, the more they send spam messages; if there are no clicks, the spam attack would be pointless and would stop.

Instead, please report that account to us immediately. To report a spammer account, please follow these steps:

On Android

- Open the other user's profile
- Tap the ... icon on the upper right corner
- Select Report
- Choose a reason for reporting and use the comment field to tell us why you're reporting that user
- Submit your report by tapping OK

On iOS

- Open the other user's profile
- Tap the ... icon on the upper right corner
- Select Report
- Choose a reason for reporting and tap Report
- In the comment field, tell us why you're reporting that user
- Submit your report by tapping Done

On Web

- Open the other user's profile
- Tap the : icon right next to the Follow button
- Select Report
- Choose a reason for reporting and use the comment field to tell us why you're reporting that photo
- Submit your report by clicking Report

It's also important that you choose a very strong password. These are made of upper case letters, lowercase letters, numbers, and symbols – all in random order. Here are some examples (do not use them!):

1. {7!Qb_8\$LS8e7@AiX22%
2. JpL9\$6xujuB[qsVt

Both spam and phishing are related to social engineering, a general term for any activity in which an attacker is trying to

manipulate you into revealing personal information. Passwords, account credentials, social security numbers--you should always think twice before giving out this information. Always verify who is really on the other end of the line.



What is a drive-by attack?

- A drive-by attack, also known as a drive-by download attack, refers to a cyberattack in which a malicious script causes a program to download and install itself on a user device, without explicit permission from the user.
- It can happen on any user device, running any operating system.
- Often, these attacks occur when the user navigates to and browses a compromised web page.
- Drive-by attacks often use exploit kits to launch the automatic download. Exploit kits are malicious pieces of software, created by hackers to identify vulnerabilities in a device, web browser, or web-based app.
- These weaknesses are then used to launch the automatic download process and carry out the attack.
- Drive-by attacks are designed to infect devices, steal information, and/or cause damage to data.

Drive-by attack methods

- Drive-by attacks are named as such because the download occurs silently.
- There are two main methods through which drive-by downloads can infect a user device:

1. Without authorization

- In these cases, there is no direct user action which causes the download to begin.
- In other words, the attack is launched when the user visits a compromised webpage, without the need for any interaction with the page, not even a single click.
- To create such an attack, the hacker injects malicious code into the web page by exploiting flaws in the website's security. When the user first visits the page, the code identifies any security vulnerabilities in either the user's web browser or the user's device, and triggers the malware download through these vulnerabilities.

2. With authorization under false pretences

- Sometimes, there is a user action involved in a drive by download, but under false pretences.
 1. There are a few different ways this can be done, for example:
A pop up advert could have an 'X' in the corner that disguises itself as a close button, but actually acts as a catalyst for starting a malicious download once pressed.
 2. A link could appear legitimate, but clicking on it could cause the download to begin.
 3. An email attachment which looks safe could actually be malicious, as part of a social engineering or phishing scheme, and clicking on it will launch the download.

All three examples involved a simple click or button press. These actions allow the attacker to claim that the user authorized the download, when in reality the user did not realize the implications of their actions, as the true intentions of the

attacker were hidden. In this way, the hacker can get away with the download without being detected.