E

Exploit Kit: How Drive-By Malware Attacks Work

An exploit kit is a malicious toolkit that profiles a visiting device, selects a matching software vulnerability, and delivers malware. Learn the redirect-to-payload chain, warning signs, investigation steps, and prevention controls.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 19, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How an exploit-kit attack works
02 Exploit kit vs. related terms
03 Possible signs and telemetry
04 What to do after suspected exposure
05 Prevention priorities
06 Frequently asked questions

An **exploit kit** is a malicious toolkit containing multiple exploits for software vulnerabilities. It profiles a visiting device, selects an exploit likely to work, and attempts to deliver a malware payload. Exploit kits historically targeted browsers and plugins through compromised websites and malvertising, enabling a drive-by infection with little or no deliberate download interaction.

An exploit kit is not the final malware. It is an automated delivery system. The installed payload might be ransomware, an information stealer, a banking Trojan, or a remote-access tool.

01 How an exploit-kit attack works

1. **Traffic source:** a compromised site, malicious advertisement, injected script, phishing link, or redirect sends the browser into an attacker-controlled chain.
2. **Gate:** the infrastructure filters visitors by location, browser, referrer, IP reputation, or previous visits to avoid researchers and unsuitable targets.
3. **Landing page:** scripts fingerprint the operating system, browser, plugin versions, and other environment details.
4. **Exploit selection:** the kit chooses code for a matching software vulnerability, often one already fixed by a vendor.
5. **Exploitation:** malicious content triggers memory corruption or another flaw and executes code outside the intended browser workflow.
6. **Payload:** shellcode or a loader retrieves and starts the final malware.
7. **Cleanup and redirection:** the campaign may redirect the user to a normal page and rotate domains to conceal the chain.

02 Exploit kit vs. related terms

Term	Meaning
Vulnerability	A weakness in software or configuration
Exploit	Code or technique that takes advantage of a vulnerability
Exploit kit	Infrastructure bundling discovery, targeting, multiple exploits, and payload delivery
Drive-by download	An unintended download or execution triggered through browsing

Term	Meaning
Fake update	Social engineering that asks the user to install something; it may not exploit a software flaw

A browser download appearing after a visit does not automatically prove an exploit succeeded. Review process and security telemetry for actual execution.

03 Possible signs and telemetry

- A chain of rapid redirects through unfamiliar advertising or newly registered domains.
- Obfuscated script, fingerprinting, or exploit content blocked by browser or network security.
- A browser or document reader spawning a script host, shell, loader, or unknown executable.
- A crash followed by a new process, file, persistence item, or outbound connection.
- Alerts naming an exploit, CVE, landing page, shellcode, or downloaded payload.
- Several users reaching the same URL but only unpatched devices becoming infected.

04 What to do after suspected exposure

1. **Isolate an affected endpoint** if payload execution is possible.
2. **Preserve the chain:** original URL, referrer, redirects, timestamps, browser version, process tree, downloaded files, DNS, proxy, and endpoint alerts.
3. **Identify the vulnerability and payload.** The blocked exploit and installed malware require different containment actions.
4. **Run a trusted full scan** and hunt for persistence, credentials accessed, and connections made after the browser event.
5. **Apply the vendor patch** across every affected product and similar endpoint. Blocking one campaign domain does not close the vulnerability.
6. **Reimage when integrity is uncertain,** especially if code executed with elevated privilege.

05 Prevention priorities

Enable automatic updates for the operating system, browser, document readers, and extensions; remove unsupported plugins and software; and prevent ordinary browsing with administrator privileges. Use exploit protection, endpoint behavior monitoring, protective DNS, web filtering, and ad-security controls. Organizations can use browser isolation for high-risk browsing and restrict browsers from launching unnecessary script interpreters or executable content.

Exploit kits are less dominant than during the era of Flash and Java browser plugins, but the model remains relevant: automate target profiling, exploit an exposed weakness, and deliver a chosen payload.

06 Frequently asked questions

Do exploit kits only use zero-day vulnerabilities?

No. They often target known vulnerabilities for which patches already exist because many devices remain outdated.

Can visiting a legitimate website expose me?

Yes. A compromised site or malicious advertisement can redirect visitors without the site owner’s knowledge. A fully patched, isolated, and monitored browser reduces the chance that exposure becomes execution.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com