

DriveSurge Turns Trusted Websites Into ClickFix Malware Traps

By GridinSoft Malware Research Team

Published: 2026-05-31 · Archived: 2026-06-04 02:00:40 UTC

A new DriveSurge campaign shows how a normal website visit can turn into a malware-installation prompt without the site owner or visitor realizing what happened. Silent Push researchers reported that the actor has compromised thousands of legitimate websites and routes selected visitors through zTDS, an open-source traffic distribution system, toward fake browser updates and ClickFix-style command prompts.

This matters for Trojan Killer readers because the first touchpoint is not a strange download portal. It can be a real business, local organization, professional services site, or other trusted page that silently loads injected JavaScript in the background. The malware step appears later, after the visitor has already trusted the website.

What DriveSurge Is Doing

According to [Silent Push's DriveSurge research](#), the activity looks like an initial-access broker operation. The actor compromises legitimate websites, injects scripts, profiles visitors through zTDS, and sends likely victims to a payload page. Silent Push says the activity fits a pay-per-install model, where successful infections become leads for downstream threat actors.

The campaign has two main delivery paths:

- **Fake browser updates.** Visitors see a convincing update page for Chrome, Firefox, Edge, Safari, Opera, Brave, Yandex, Vivaldi, Samsung Internet, UC Browser, or a generic browser category. In one analyzed case, a fake Firefox page downloaded a ZIP file containing DLLs and `Browser Update.exe`.
- **ClickFix prompts.** Visitors see a fake error or repair message that tells them to copy and paste a command into PowerShell or a terminal. Silent Push observed one ClickFix instance trying to retrieve malicious code from `91.92.240[.]127`.

Both paths abuse everyday trust signals: a familiar website, a familiar browser, and a message that sounds like maintenance. The safest assumption is that browser updates should never come from a pop-up on a random website, even when that website itself is legitimate.

Technical Clues Worth Checking

Signal	What to look for	Why it matters
Campaign name	DriveSurge	Use this term when searching incident notes, proxy logs, browser history,

Signal	What to look for	Why it matters
		and endpoint alerts.
Traffic system	zTDS and jsrepo request patterns	Silent Push tied the redirects to zTDS infrastructure and malicious JavaScript injection chains.
Fake update file	Browser Update.exe inside a ZIP archive	A browser should update through its built-in updater or official store, not a downloaded ZIP from a web prompt.
Reported ZIP hash	90aecb370dfb1a99a1f7de0a9c6842ab1b664521fddea16b0ec9a91f322646fc	This SHA256 can help defenders search file inventories and endpoint telemetry.
ClickFix network clue	91.92.240[.]127	Silent Push observed a ClickFix chain attempting to pull code from this IP address.
Injected script style	t.js , t.<12 hex chars>.js , ext-b<12 hex chars>.js	These script-name patterns were part of the infrastructure fingerprints used to map DriveSurge.

Trojan Killer browser cleanup

Pop-ups came back after you blocked the site?

Recurring redirects usually mean a permission, extension, policy, or bundled app is still present. Clean browser settings first, then scan Windows if the prompts return.

- Checks browser changes
- Finds bundled malware
- Online scanner available

What to Do If You Saw a Fake Update or ClickFix Prompt

- **Do not run the command.** If a page tells you to paste a PowerShell or terminal command, close the tab. A real browser repair step should not ask for that.
- **Do not open the downloaded ZIP or EXE.** Delete nothing yet if this is a work device; preserve the file name, download time, URL, and browser history for review.
- **Disconnect if you launched it.** If `Browser Update.exe` or another suspicious installer ran, disconnect the device from the network before signing in to more accounts.
- **Check browser history and downloads.** Look for the legitimate site you visited, followed by redirects, fake update pages, ZIP downloads, or PowerShell-copy instructions.
- **Review startup points.** After a fake update runs, inspect startup apps, scheduled tasks, browser extensions, and recently modified files under user profile paths.
- **Change passwords from a clean device.** Prioritize email, password manager, Microsoft, Google, banking, crypto, and workplace accounts if the suspicious file executed.

For Windows cleanup, follow a full process instead of only deleting the downloaded file. The [Trojan Killer malware removal guide](#) covers the practical cleanup order, and [Trojan Killer](#) can scan the system after the device is isolated. If the lure involved a copied command, also review the related [ClickFix PowerShell guide](#).

If You Own a Website

DriveSurge is also a website-owner problem. A compromised site may look normal to admins while non-admin visitors receive injected scripts. Silent Push documented logic that avoids WordPress administrator sessions, which means an owner can miss the infection during a routine logged-in check.

- Test the site from a clean browser profile while logged out of WordPress.
- Search page source, access logs, and file integrity alerts for unfamiliar externally loaded JavaScript.
- Investigate requests involving `jsrepo` , `t.js` , strange 12-character hex JavaScript names, or newly added domains.
- Patch CMS, plugin, theme, and server software before cleaning injected code.
- Rotate admin, hosting, FTP/SFTP, database, and CDN credentials after removing the compromise.

Gridinsoft's [Website Reputation Checker](#) can help triage suspicious domains found during cleanup, but it should not replace a source-code and server-log review.

How to Avoid This Attack Path

- Update browsers only through the browser's built-in update screen or an official app store.
- Never paste a command from a web page into PowerShell, Terminal, or Run.
- Treat fake update pages, fake CAPTCHA pages, and clipboard-based fixes as related social-engineering patterns.
- Use script-blocking or DNS filtering where it does not break required work, especially for unmanaged browsing on business systems.
- Train users to report a suspicious prompt even when it appeared on a trusted website.

The same pressure tactic appears in [fake CAPTCHA scams](#) and other ClickFix pages: the browser message claims there is a simple problem, then asks the user to perform the malware installation step. DriveSurge expands that pattern through compromised websites and traffic routing infrastructure.

Bottom Line

DriveSurge is not just another fake-update page. The important part is the delivery chain: trusted sites, hidden redirects, zTDS filtering, and social-engineering pages that adapt to the visitor. If you saw a fake update or ClickFix prompt after visiting an ordinary site, treat the device as exposed until downloads, browser history, startup entries, and endpoint telemetry have been checked.

Related security guides

[Browser Notification Spam and Redirects: Cleanup Guide](#) May 26, 2026

[Sessionverify.co.in Pop-up Ads and Browser Spam](#) May 24, 2026

[Snconor.vg Pop-ups: Browser Notification Spam and Redirect Cleanup](#) May 24, 2026

[Click Allow To Verify Session: Fake CAPTCHA Notification Scam](#) May 25, 2026

Source: <https://trojan-killer.net/drivesurge-clickfix-fake-browser-updates/>