Fake Zillow pages use ClickFix NetSupport RAT to target apartment hunters

By Mirko Zorz

Published: 2026-11-12 · Archived: 2026-11-14 02:00:22 UTC

EfficientIP Research Labs traced a ClickFix campaign that used fake Zillow apartment-review pages to install NetSupport RAT on visitors' Windows computers.



Each page showed what looked like a routine verification check. Behind it, the page quietly copied a PowerShell command to the clipboard and walked the visitor through pasting and running it. Doing that installs remote-control software that keeps its window hidden and starts back up every time the user logs in.

Renters are the people most at risk, and so is anyone who checks listings on a work laptop. Once NetSupport is running, an attacker can reach any file the logged-in user can reach. EfficientIP detected the first domains in August 2026.

Three keys and you're done

ClickFix is a social engineering trick that gets users to pass a fake check by running a command themselves. On these pages, clicking Continue loaded the clipboard, and the instructions read Win+R, Ctrl+V, Enter. The command fetched a script from an IP address written as a decimal number, 1495423691, which converts to 89.34.90.203.

The script hid its PowerShell window and used a Python runtime it downloaded to pull a ZIP archive from the same address. It unpacked NetSupport into AppData and dropped a shortcut in the Windows Startup folder. NetSupport Manager is legitimate remote administration software. The attackers used it for the job it was built for, on computers owned by people who thought they were reading apartment reviews.

How the links probably got out

The researchers worked from the infrastructure side and did not see how victims reached the pages. Karim Hossen, the company's CISO, offered an assessment.

"Most likely: links sent directly to targets, probably in a rental listing scam context (e.g. a fake landlord or agent sending a "check the reviews / verify before the visit" link by email, SMS or messaging app)," he told Help Net Security.

"The domains were newly registered, short-lived and used random numeric suffixes (e.g. apartments-review8509831[.]sbs). They also used wildcard subdomains (*.verify.apartments-review[.]sbs), which are typical of unique per-target or per-campaign links."

He rated malicious ads and redirect chains less likely, because the researchers saw no evidence of an ad or redirect layer. He rated search poisoning least likely of all. "Throwaway domains with random numbers that lived only a few days would rarely appear in search results, and nobody would type them manually."

If he's right, the red flag shows up before you ever see the page. It's the message from someone who says they've got the perfect apartment and just need you to click one link first.

Digging up the rest

EfficientIP first spotted a handful of these domains in its passive DNS data, which logs which names resolved to which addresses over time. The names all followed one pattern: apartments-review plus digits, on the .sbs top-level domain. Live DNS records told the researchers little, because the domains lived briefly and sat behind Cloudflare, which hid the hosting.

The researchers then searched Certificate Transparency logs, the public record of issued TLS certificates, and found domains that were missing from their DNS data. The domains did not consistently share nameservers and resolved to different Cloudflare addresses. The pages still gave them away: they used the same fake Zillow template, the same encoded IP and download path, and the same NetSupport deployment.

The installed NetSupport client pointed to two gateway domains, asgomd[.]com and asgrsv[.]com. "Pivoting on their IP addresses revealed seven additional domains following the same short naming pattern (e.g. bksju, decrmd, jpgomd, nogomd, decrsv, jpgrsv)," Hossen said. "Their shared "-md"/"-rsv" suffixes suggest they were registered as a single set of gateway infrastructure for this operator."

The researchers have not tied the operator to a known group. "NetSupport RAT is widely abused with cracked or reused licenses across many unrelated actors, so license strings alone are a weak attribution signal unless they match a documented cluster," Hossen said. "We consider this activity part of the broader ClickFix/NetSupport ecosystem rather than an attributed campaign."

Source: https://www.helpnetsecurity.com/2026/11/13/fake-zillow-clickfix-netsupport-rat/