CRXFILTRATE / MAY 2026

How one anomaly became a 16-month browser extension cluster that bypassed every defense layer.

01

ANOMALY

Permissions didn't match

A 7AI researcher reviewed a color picker. The requested permissions didn't fit the stated function. One sandbox spin-up confirmed a JavaScript execution backdoor running in every page.

02

INVESTIGATION

A factory came into view

Threat Research mapped 22+ extensions across three browser stores, ~60 active domains, a versioned release pipeline, and seven new C2 domains added three days before publication.

03

HUNT

Agents ran the sweep

7AI agents ran the IOC sweep across DNS, proxy, network, and extension telemetry in customer environments. The standard EDR-plus-proxy-plus-DNS stack had seen nothing actionable.

04

TRIAGE

Context already assembled

Where exposure surfaced, the customer's AI Security Engineer moved into triage with the full investigation context already built. No wait for publication. The hunt was already running.

22+
malicious extensions

85K+
documented installs

16+ mo
active and expanding

3
browser ecosystems

PLAID ELITE

Threat research + the hunt + your environment.