SALES BRIEF / FOR PROSPECT DISTRIBUTION

The browser extension cluster that ran past every defense layer for sixteen months.

7AI Threat Research uncovered an active, three-platform malicious extension factory delivering attacker-controlled JavaScript into authenticated corporate browser sessions. EDR didn't catch it. Web proxies didn't catch it. DNS protection didn't catch it. PLAID ELITE found it live in customer environments.

22+
Malicious extensions across Chrome, Edge, and Firefox

85,000+
Documented installs as a conservative floor

16+ mo
Active and expanding since Palant's January 2025 disclosure

3
Browser ecosystems (Chrome, Edge, Firefox)

WHAT WE FOUND

- **A JavaScript execution backdoor, not adware.** The cluster strips CSP headers and injects attacker-controlled JavaScript into every page the user visits. Today's payload is ad fraud. The architecture supports anything the operator delivers next: credential capture on SSO, session theft on banking, token injection on admin consoles.
- **A factory, not a one-off.** Twelve compartmentalized developer accounts, a versioned release pipeline, internal project-tracker tickets above MM-390, and the same architectural template across every extension. Seven new C2 and ad-delivery domains added three days before publication. Three confirmed cluster extensions remained installable at paper validation.
- **A second delivery vector the install count misses.** The cluster also delivers via third-party tracker chains on legitimate websites. Endpoints with no extension installed are still exposed. The install base is one input, not a ceiling.
- **A detection gap the standard stack can't close.** No dropped files, no new processes, no registry keys. The browser making normal-looking requests to domains the categorization databases haven't seen. An endpoint sensor flagged the DNS query as suspicious in raw telemetry. The pipeline above it never promoted the signal to an alert.

WHY THIS MATTERS TO ENTERPRISE TEAMS

The cluster's disguises are consumer categories: color pickers, ad blockers, screen capture, font tools. Install counts reflect consumer behavior. The enterprise exposure comes from the same browsers and the same identities being used at work the next morning. The consumer install count isn't the ceiling on enterprise exposure. **It's the floor.** When 7AI walked enterprise security teams through evidence in their own telemetry, none of them treated this as niche extension cleanup. They treated it as a live incident.

> One endpoint sensor flagged the DNS query as suspicious in raw telemetry but the detection pipeline above the sensor never promoted it to an alert a SOC analyst would actually see. The signal existed; the surfacing failed. That's the gap proactive hunting against raw telemetry closes.
>
> 7AI THREAT RESEARCH / MAY 2026

HOW 7AI SURFACED THIS

1. A 7AI researcher reviewed a color picker before installing it. Permissions didn't match the stated function.
2. Sandbox analysis confirmed the backdoor. Source review mapped the full extension architecture and C2 infrastructure.
3. PLAID ELITE ran the IOC sweep across customer environments. Where exposure surfaced, the customer's AI Security Engineer was in triage with context already assembled.

THE PLAID ELITE DIFFERENCE

7AI's agents handle the volume of IOC sweeps across DNS, proxy, network, and extension telemetry. Engineers handle per-environment judgment. Your AI Security Engineer triages with context already assembled. The hunt is already running.

Would your current stack catch what we caught?
Run this hunt against your environment.

START THE CONVERSATION
7ai.com/contact