CRXfiltrate — IOC Block List

CLASSIFICATION	**TLP:AMBER**
PREPARED BY	7AI Threat Research Team
LAST UPDATED	2026-05-12

ABOUT THE NAME

CRXfiltrate is 7AI's name for this campaign. The underlying extension cluster was first publicly documented by Wladimir Palant in January 2025 as **Phoenix Invicta**; that name is preserved where it ties to his original research for continuity. Customers who received the V3 IOC blocklist under the Phoenix Invicta name are looking at the same campaign — this is the V4 update under the public name. The public research is available at `https://7ai.com/crxfiltrate`.

How to read this document

- **Run the IOC sweep before the extension inventory.** A clean extension audit does not rule out exposure. The cluster also delivers via third-party tracker chains on legitimate websites with no extension installed on the host. Page-served exposure shows up in DNS and proxy logs even when the endpoint has no malicious extension. Run both hunts against the same lookback window.
- The IOCs below are organized by infrastructure cluster and confidence tier. Higher tiers are higher-confidence and lower-noise.
- Where an IP is annotated **Host/SNI scope only** or "shared", do not block by IP alone — block by domain, Host header, or SNI to avoid collateral on legitimate co-tenants.

1. Domains — BLOCK

All domains below are exclusively used by the threat actor unless otherwise marked. Block at proxy, firewall, or DNS resolver.

Critical — JavaScript Execution Backdoor and C2

DOMAIN	RESOLVES TO	ROLE
`statsdata.online`	`5.149.255.43`	Primary JavaScript execution backdoor
`secdomcheck.online`	Host/SNI scope only	Backup execution backdoor — do not block by IP; use domain, Host, or SNI
`lottingem.com`	`5.149.249.219`	C2 round-trip endpoint (data exfiltration in URL, payload in response body)
`fivestat.com`	`5.149.255.43`	Production payload host (`m3011.js`)
`datvault.cloud`	Path-scoped: `/c`, `/logb.php`	Event telemetry + distributed reconnaissance (DOM intelligence gathering)
`doublestat.info`	`5.149.249.216`	Identity-harvester exfiltration target (variant-gated capability)
`shurkul.online`	`5.149.255.43`	Script-delivery server (path-rotating: `/v1712/g1001.js` → `/v1713/g1001.js`)
`singleview.site`	`5.149.249.216`	Tracking/config infrastructure
`gadstat.com`	`5.149.255.43`	Cluster A C2 infrastructure
`sevendata.fun`	`5.149.255.43`	Cluster A C2 infrastructure (added 2026-05-11)
`marsdata.online`	`5.149.255.43`	Cluster A C2 infrastructure (added 2026-05-11)
`8melo.fun`	`98.142.252.135`	Gen 2 C2
`hjk-9l.cloud`	`98.142.252.185`	Gen 2 C2

High — Tracking, Ad Injection, Data Exfiltration

DOMAIN	RESOLVES TO	ROLE
everyview.info	5.149.249.216	Extension config server
doubleview.online	5.149.249.219	Impression tracking
gulkayak.com	5.149.249.218	Ad content delivery
triplestat.online	5.149.255.43	Click monetization
topodat.info	5.149.255.43	Click analytics
searchresultslist.online	5.149.249.218	Search / ad delivery infrastructure (added 2026-05-11)
nocodata.online	5.149.249.219	Cluster A secondary infrastructure (added 2026-05-11)
locodata.site	5.149.249.219	Cluster A secondary infrastructure (added 2026-05-11)
youtube-ads-skip.site	5.149.249.219	Cluster A secondary infrastructure (added 2026-05-11)
dailyview.site	5.149.249.216	Tracking / config infrastructure (added 2026-05-11)
rumorpix.com	5.149.249.x	Iframe content
astralink.click	Gen 2	Click attribution / redirect
astato.online	referenced	Tracking / dormant
aj2472.online	referenced	Epom proxy / dormant

High — Extension Config Servers

Any DNS resolution to these domains confirms the matching malicious extension is installed on the endpoint.

```
super-sound-booster.info → Volume Booster
adblock-ads-and-yt.pro → AdBlock · Ads/YT
screencapx.co → ScreenCapX
manuals-viewer.info → Manuals Viewer
skip-n-watch.info → AdBlock Skip-n-Watch
capture-it.online → Capture It
easy-dark-mode.online → Easy Dark Mode
skipadsplus.online → SkipAds Plus
font-expert.pro → Font Expert
megaboost.site → Undocumented (volume booster)
speechit.pro → Undocumented (text-to-speech)
video-downloader-plus.info → Config server
best-browser-extensions.com → Distribution / install funnel
1-click-cp.com → 1-Click Color Picker (Gen 2)
pixel-pick.pro
yk7-j3.space
poiuy.fun
lop5i.fun
mn8p-q.fun
loudmax.net
ab-c1d.info
as-dfg.online
efg2h.pro
hjklm.site
gf-dsa.space
qw-ert.space
trw-4s.space
```

Medium — Search Monetization Infrastructure

Domains in this tier are part of the operator's monetization chain but are operationally entangled with legitimate search-monetization infrastructure. The operator routes through these platforms as a publisher; the platforms themselves are not exclusively operator-controlled. Block in the context of cataloged extension traffic; treat as shared services rather than actor infrastructure when scoping policy.

```
itonsearch.com
cdn.itonsearch.com
u.itonsearch.com
beacon.itonsearch.com
seccint.com
beacon.seccint.com
sns-p-search-event-tracker-us-east-1-k8s.seccint.com
se-p-static-content.seccint.com
rdr-performance-p.seccint.com
idp-cf.com
onclckbnr.com
www1.softy.org → Fake Google SERP (45.55.78.246)
somavar.com → Fake Bing SERP (44.230.5.79)
domain-error.com → Original SERP template (45.79.167.180)
```

CDN — Block by URL Path Only (DO NOT block the bare domain)

The domain `ahacdn.me` is a shared CDN with legitimate ad networks as co-tenants. Block at the path level only.

ACTION	INDICATOR	NOTES
BLOCK	`cdn23602612.ahacdn.me`	Actor-specific subdomain — safe to block
BLOCK	`Any URL containing /500b-bench.jpg on ahacdn.me`	**Highest-signal indicator in this campaign — zero FP**
BLOCK	`cdn19034103.ahacdn.me`	Ad content delivery — safe to block
DO NOT BLOCK	`ahacdn.me bare domain`	Shared with legitimate ad-tech
DO NOT BLOCK	`cdn31530260.ahacdn.me`	Legitimate: SelectMedia / Bidmatic
DO NOT BLOCK	`cdn53833466.ahacdn.me`	Legitimate: Adtelligent
DO NOT BLOCK	`unocdn.com`	Legitimate CDN proxy

2. IPs — BLOCK with care

ACTION	IP	NOTES
BLOCK	`5.149.255.43`	HZ-Hosting Bulgaria — primary cluster IP (~9 actor domains co-resolve)
BLOCK	`5.149.249.216`	HZ-Hosting Bulgaria — actor infrastructure
BLOCK	`5.149.249.218`	HZ-Hosting Bulgaria — actor infrastructure
BLOCK	`5.149.249.219`	HZ-Hosting Bulgaria — actor infrastructure
BLOCK	`79.141.164.251`	Per-extension config server
BLOCK	`98.142.252.135`	Gen 2 C2
BLOCK	`98.142.252.185`	Gen 2 C2

DO NOT block these IPs by themselves

IP	REASON
`93.123.17.252`	Co-tenants include Microsoft / Gcore CDN (`msedge.b.tlu.dl.delivery.mp.microsoft.com`). Identified as a known false positive — do not use as standalone IOC
`45.133.44.0/24`	Shared with legitimate ad networks
`88.208.5.12`	Same shared-hosting concern

For these shared addresses, enforce by actor Host header, SNI, or URL path — not by IP.

3. Browser Extensions — FORCE REMOVE and BLOCK INSTALLATION

Chrome Extension IDs (20 confirmed + 1 lower-confidence ledger-only)

EXTENSION ID	NAME
`jckoejjnaljgkmgblmbodoegoefofhee`	MyColorPick
`fmpgmcidlaojgncjlhjkhfbjchafcfoe`	1-Click Color Picker
`gpibachbddnihfkbjcfggbejjgjdijeb`	Better Color Picker
`aplhgigkopkholapijailboandapfaim`	ColorPickPro
`nonajfcfdpeheinkafjiefpdhfalffof`	AdBlock — Ads and YouTube
`coebfgijooginjcfgmmgiibomdcjnomi`	AdBlock for YouTube: Skip-n-Watch
`ihfedmikeegmkebekpjflhnlmfbafbfe`	ScreenCapX
`lkalpedlpidbenfnnldoboegepndcddk`	Capture It
`nbljjljaoanknannhlonmaknhckcoldi`	SimpleSnap
`jlpchojjamcikhgmedobmfodcefjmccn`	SnipCapture
`pnhkolkelkfnfphohbdnboedhejlfbho`	RecItEasy
`ojkoofedgcdebdnajjeodlooojdphnlj`	Volume Booster
`mkoegjeakpnbjklhimnimkgokbifeaoh`	ExtraSound Volume Booster
`ibbkokjdcfjakihkpihlffljabiepdag`	Easy Dark Mode

EXTENSION ID	NAME
`ieihbaicbgpebhkfebnfkdhkpdemljfb`	Manuals Viewer
`ocbfgbpocngolfigkhfehckgeihdhgll`	Manual Finder 2024
`pjlheckmodimboibhpdcgkpkbpjfhooe`	Font Expert
`acbcnnccgmpbkoeblinmoadogmmgodoo`	Click & Pick
`ekafoahfmdgaeefeeneiijbehnbocbij`	Dopni: Automatic Cashback
`emnhnjiiloghpnekjifmoimflkdmjhgp`	SkipAds Plus
`mmjhombiehngfpipefodkebphfnblphe`	Ledger-only entry (**LOWER CONFIDENCE** — telemetry co-occurrence only; require surrounding context before action)

Edge Extension IDs

EXTENSION ID	NAME
`bkknccgnmpcnhppklomdjkphccmpblga`	1-Click Color Picker: Instant Eyedropper
`jbdegnmcajkhjemebonejojlgkgcddhc`	AdBlock for YouTube: SkipAds

Separately-Operated Finding — DO NOT roll into this cluster's metrics

This extension is independently malicious but operated by a **different threat actor**. Track separately and apply attribution hygiene — it belongs in its own bucket, not in this cluster's IOC set.

EXTENSION ID	DETAILS
`gogbiohkminacikoppmljeolgccpmlop`	Color Picker — Eyedropper (~400,000 users, Cloudflare infrastructure, AES-encrypted exfil to `colorspicker[.]net`; prior public attribution: Annex Security, 2024)

4. Detection Patterns — ALERT

Use these patterns in proxy logs, SIEM, or network monitoring. Listed in order of detection confidence.

PRIORITY	PATTERN	WHAT IT DETECTS
HIGHEST	Any URL request containing `/500b-bench.jpg` on `ahacdn.me` subdomains	Production payload connectivity probe — operator-specific URL pattern, highest-fidelity indicator in this campaign
HIGH	Any request to `cdn23602612.ahacdn.me`	Actor-assigned CDN subdomain
HIGH	POST to `*/c` with base64-encoded body from a browser process to an uncategorized domain	C2 heartbeat — survives domain rotation
HIGH	POST to `*/alk/g2.php`	JavaScript execution backdoor endpoint
HIGH	GET to `*/re.php?mk=doublestat`	C2 round-trip with full page title in URL (exfiltration in URL parameter; response-blocking does not prevent surveillance)
HIGH	URL path matches `*/mva_v*/m3011.js` or `*/nva_v*/m3011.js`	Production payload delivery
MEDIUM	POST to `*/logb.php` with JSON body	DOM intelligence gathering (distributed reconnaissance)
MEDIUM	GET/POST to `*/clce` or `*/agg/log/top`	Click classification and position tracking

Process scoping: expected source process is `chrome.exe`, `msedge.exe`, or another Chromium-based browser. Any non-browser process contacting these IOCs warrants its own investigation as a different threat.

5. Forensic Artifacts — Check on Compromised Endpoints

ARTIFACT	LOCATION	SIGNIFICANCE
`localStorage.gotAriaLabel`	Browser localStorage (any domain)	Confirms the identity harvester executed and the signed-in Google user's real name and email were exfiltrated to `doublestat.info`. **Note:** this capability is variant-gated — some captured payloads have it disabled, so its absence does not rule out other variant infections
`localStorage.zLastRedHer`	Browser localStorage	Timestamps when the JavaScript execution backdoor last fired
Chrome extension directories	`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\`	Check for any extension ID listed in Section 3
Edge extension directories	`%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Extensions\`	Check for any Edge extension ID

6. File Hashes (where reliable)

SHA-256	FILE	SIZE
`da60712fa0218cce2596366d6d496dc69fa9be5735c5bfcf54a5cb69b2748ab3`	`redirect_checker.js` (Gen 1)	44,003 bytes
`47dde4de0a2eac88b19452ef80ba3c1a2f5b0edfca8980dc1f2697277888bdb3`	AdBlock CRX package	986,435 bytes

Note: Most cluster payloads are uniquely customized per victim via server-side template substitution. File hashes for `m3011.js`, `g105.js`, and C2 responses are **unreliable for detection** — no two endpoints receive the same file. Detection must target behavioral patterns rather than static file signatures. YARA rules in the full paper match structural patterns rather than fixed hashes.

What's new in this version (2026-05-12)

CHANGE	IMPACT
Document renamed to CRXfiltrate	7AI's public name for this campaign; the underlying cluster remains Phoenix Invicta (per Palant, January 2025) for continuity with prior research
Added Vector B operational guidance (page-served path)	Run DNS sweep alongside extension audit; a clean extension audit no longer rules out exposure

CHANGE	IMPACT
Removed `phillbeieoddghchonmfebjhclflpoaj` from the cluster Chrome list	Analyst review resolved the suspected match to a `paletteBuilder.js` "check elements" function unrelated to the operator's identity harvester. No other cluster infrastructure indicators appear in its source — investigated and excluded (paper §5)
Fixed misclassification of `jbdegnmcajkhjemebonejojlgkgcddhc`	Moved from Chrome to Edge
Added 7 Cluster A domains	`sevendata.fun`, `marsdata.online`, `nocodata.online`, `locodata.site`, `youtube-ads-skip.site`, `dailyview.site`, `searchresultslist.online`
Updated terminology	"Remote Code Execution backdoor" rewritten as "JavaScript Execution Backdoor" — more technically precise; the backdoor executes operator-controlled JavaScript in the visited page's realm, not full system RCE
Clarified `93.123.17.252` status	Removed from blockable IOC list — known false positive (co-tenant: Microsoft / Gcore CDN). Treat as "do not block by IP"
Identity harvester	Marked as variant-gated rather than universally present

Last updated 2026-05-12 by 7AI Threat Research. Contact your account team for the latest version. The public research is available at `https://7ai.com/crxfiltrate`.