THREAT INTELLIGENCE REPORT

BoostKey / Session Export Tool

App Store Connect Credential Harvesting Operation

Feb 22, 2026 | Severity: HIGH | Status: Live at time of discovery

Researcher: Jean-Marie R. (Toborrm9)

How This Was Found

I am building a malicious browser extension detection tool that performs automated behavioral analysis on newly published Chrome extensions. On February 22, 2026, the tool flagged "Session Export Tool" (mimplmibgdodhkjnclacjofjbgmhogce) on its first day of publication. The flag was triggered by broad cookie permissions, a support domain registered only 8 days prior, and source code patterns consistent with credential harvesting.

Manual investigation of the extension source code led to boostkey.app, where reverse engineering the platform's compiled JavaScript revealed a complete 5-step fraud operation targeting Apple App Store Connect developer accounts. This finding was made on the extension's first day of publication with no prior public documentation.

Methodology

- Static analysis of extension source code and declared permissions
- Review of platform client-side JavaScript bundle via compiled chunk extraction
- Inspection of service workflow and cookie validation logic
- Live API endpoint testing in isolated sandbox environment
- No interaction with third-party user accounts

Indicators of Compromise

Field	
Extension ID	mimplmibgdodhkjnclacjofjbgmhogce
Extension Name	Session Export Tool
Domain	boostkey.app
Telegram	t.me/boostkey_support
Domain Created	2026-02-14 09:23:08 UTC
Domain Expires	2027-02-14 09:23:08 UTC
Payment	NOWPayments (crypto only, $150)
Target Cookies	myacinfo, itctx
Target Platform	App Store Connect
Collection Endpoint	/api/orders/{orderId}/cookies

Why This Is Not a Legitimate Integration

Legitimate integrations with App Store Connect use Apple-issued API keys and JWT-based authentication scoped to specific permissions. No documented Apple workflow requires extraction or transfer of browser session cookies.

Web session cookies function as bearer tokens. Possession of these values is sufficient to issue authenticated requests without password or MFA revalidation until session expiration. The Chrome cookies API with host_permissions grants access to cookies marked HttpOnly, which are intentionally protected from normal web page access. This elevated privilege is what makes the extension capable of extracting authentication tokens that standard web scripts cannot reach.

Extension Permission Analysis

Permission	Capability Enabled	Relevance to Workflow
`cookies`	Read all cookies including HttpOnly tokens	Extracts myacinfo and itctx session tokens
`activeTab`	Access current tab URL and context	Ensures extraction targets authenticated ASC session
`clipboardWrite`	Write data to system clipboard	User-mediated transfer of session payload to platform
`https://*.apple.com/*`	Scoped access across all Apple subdomains	Explicitly targets App Store Connect authentication scope

---

Attack Chain

1. Lure

boostkey.app poses as a legitimate ASO service offering "Game Center keyword injection" to boost App Store rankings. Targets are iOS developers already willing to bend Apple's rules, making them less likely to question unusual requirements.

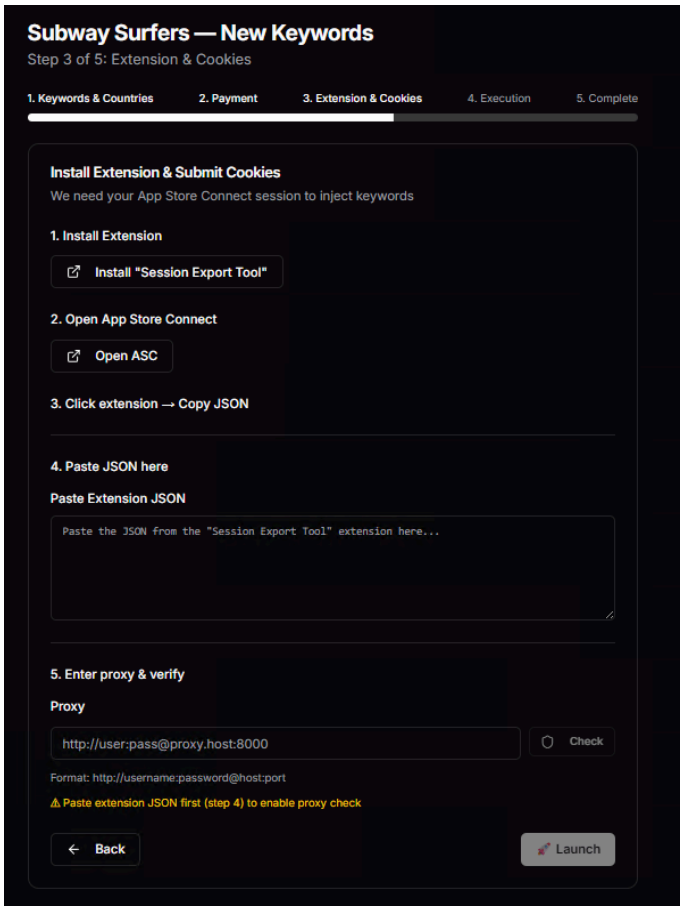
2. Payment

Developer pays $150 in cryptocurrency via NOWPayments - untraceable, non-refundable. The payment creates commitment and removes hesitation for the steps that follow.

3. Extension & Cookies (Step 3 of 5)

After payment the developer reaches a page titled "We need your App Store Connect session to inject keywords" with these instructions:

- Install Session Export Tool - direct link to mimplmibgdodhkjnclacjofjbgmhogce
- Open App Store Connect and run the extension
- Paste the copied JSON into the platform textarea
- Provide a proxy routing through their own IP
- Click Launch



4. Validation

The platform validates the pasted JSON client-side before submission, specifically requiring:

```
if (!a.includes("myacinfo")) throw Error("Missing required cookie: myacinfo");
if (!a.includes("itctx")) throw Error("Missing required cookie: itctx");
```

These are the two primary App Store Connect session tokens. This function enumerates all cookies for the specified domain and includes their raw values in the returned structure. Because the extension executes with elevated privileges, this allows access to cookies marked HttpOnly, which are intentionally protected from normal web page access.

5. Session Replay via Proxy

The platform requires the developer to supply an HTTP proxy routing through their own IP address. This allows subsequent requests using the exported session to originate from infrastructure controlled by the service operator rather than the developer's browser, while appearing to Apple's systems as originating from the developer's known location.

Impact

A valid App Store Connect session obtained through this workflow permits all actions available to the authenticated account:

- Full access to all apps in the compromised developer account
- Application management and build submission including app updates pushed to existing users
- Access to Apple Developer certificates and provisioning profiles
- Distribution of builds via TestFlight
- Access to billing and personal account information
