

Section 7

Steam Web API endpoints used in the hijack pattern

Investigated by: Agent Amy

Steam Web API endpoints used in the hijack pattern

The endpoints behind the sequence.

Context & source limits

These are the Steam Web API endpoints that the reported hijack scripts used to intercept trades without passing through the browser-side confirmation steps.

Four documented endpoints do the whole job. None of them is a flaw, none needed exploiting — a valid key calls them and Steam answers. **The key is the only thing the attacker had to steal.**

IEconService / GetTradeOffers / v1 POLLING

Used to monitor the account's trade offers. Scripts poll this endpoint repeatedly with the compromised API key; it returns the details of newly created, pending or modified trade offers. Polling intervals are not measured here.

Threat vector: Discloses pending trade offer IDs and the recipient's profile details.

IEconService / CancelTradeOffer / v1 INTERACTION

Used to programmatically invalidate the user's legitimate trade offer. Before 2023 no step-up authentication protected the key, so an automated server could cancel an offer as soon as it was detected, without any prompt to the account holder.

Threat vector: Voids the trade before the account holder completes the mobile confirmation.

ISteamUser / GetPlayerSummaries / v2 RECON

Queried to retrieve the profile name, avatar image URL and level of the legitimate trade recipient. This lets the script dress a prepared clone account to match. No timing is measured here.

Threat vector: Supplies the data needed to impersonate the intended recipient.

/dev/ajaxregisterkey CREATION

Steam's registration endpoint for keys. Historically, any active browser cookie session (‘steamLoginSecure’) could register a key without a Steam Guard confirmation on the mobile device, and without any notification to the account holder.

Threat vector: A persistent credential created by a script, unseen by the account holder.

[Download PDF](#)

[Download JSON](#)

[Download PGP signature](#)

PhishDestroy · file integrity signature for this fact

[Material record ↗](#)