QueenWatcher - Web Risk Profiler

Reference Guide

Overview

QueenWatcher is a browser extension designed to act as an additional layer of security awareness while you browse the web. It analyzes webpages in real-time and provides a risk score (0-100) based on various technical indicators that are commonly associated with phishing attempts, social engineering attacks, and other malicious activities.

QueenWatcher is not an antivirus, firewall, or a substitute for safe browsing practices. It is best understood as a vigilant companion that highlights elements on a webpage that *might* warrant closer inspection and should raise your alert level.

How It Works

When you visit a webpage, QueenWatcher examines the page's structure and behavior, looking for patterns and technical indicators that are frequently used in cyberattacks. It combines these observations into a single, easy-to-understand risk score:

Risk Level	Score Range	Badge Color	Meaning
Safe	0-20	Green	No significant risk indicators detected
Low Risk	21-50	Yellow	Some minor indicators present
Medium Risk	51-75	Orange	Several indicators warrant attention
High Risk	76-100	Red	Multiple serious indicators detected

Clicking the QueenWatcher icon in your browser toolbar opens a popup that shows:

- The overall risk score for the current page
- A breakdown of specific findings
- Explanations of what triggered each alert

What QueenWatcher Detects

1. Form-Based Phishing Indicators

QueenWatcher examines HTML forms on the page and flags:

- Forms that submit data (especially passwords) to external domains
- Form actions pointing to suspicious top-level domains (TLDs)
- Domain names that closely resemble legitimate sites (homograph attacks)
- Randomly generated domain names often used in phishing campaigns

2. Browser-in-the-Browser (BitB) Attack Patterns

BitB attacks create fake browser windows or login popups using iframes.
QueenWatcher looks for:

- Full-screen iframes that overlay the page
- Iframes mimicking popular login providers (Google, Microsoft, Apple, etc.)
- Suspicious positioning and styling that mimics legitimate popups
- Cross-origin iframes with hidden borders or disabled scrolling

3. Suspicious Script Activity

JavaScript can be used maliciously in various ways. QueenWatcher checks for:

- Heavily obfuscated scripts (high entropy code)
- Scripts loaded from external or suspicious domains
- Overrides of native browser functions (eval, document.write, etc.)
- Content Security Policy (CSP) violations

4. Fake CAPTCHA Detection

Fake CAPTCHAs are increasingly used to trick users into:

- Running malicious commands (e.g., "Press Windows+R, then Ctrl+V")
- Enabling browser notifications that push malware
- Downloading malicious files disguised as "verification"

QueenWatcher flags CAPTCHA implementations that:

- Use CAPTCHA branding without legitimate provider scripts
- Include suspicious instructions to run commands or enable permissions

- Request notification permissions in unusual contexts

5. Suspicious Download Triggers

Automatic or hidden downloads are a common malware delivery method. QueenWatcher detects:

- Hidden links with download attributes pointing to executable files
- Blob/data URLs that might trigger automatic downloads
- Programmatic download attempts via JavaScript

6. Dynamic Content Monitoring

Modern malicious pages often inject harmful content after the initial page load. QueenWatcher uses a MutationObserver to continuously watch for:

- Dynamically added forms (especially login forms)
- Injected iframes
- New scripts added to the page
- Changes to existing elements that make them suspicious

Important Limitations

False Positives Are Possible

QueenWatcher uses heuristic analysis, meaning it looks for patterns rather than confirming actual threats. A complex, legitimate webpage may trigger warnings because:

- Large web applications often load scripts from multiple domains
- Legitimate services may use iframes for embedded content
- Modern web apps frequently use obfuscation for code protection
- Some sites use custom CAPTCHA implementations
- Legitimate downloads (like PDFs or documents) may match suspicious patterns

A high-risk score does not necessarily mean a page is malicious. It means the page contains technical elements that *could* be used maliciously. Always use your judgment.

False Negatives Are Also Possible

Conversely, QueenWatcher may miss sophisticated attacks because:

- Attackers constantly evolve their techniques
- Some malicious code is indistinguishable from legitimate code
- Social engineering attacks may not involve any technical indicators
- Encrypted or heavily obfuscated content may evade detection

A low-risk score does not guarantee a page is safe. Always be cautious when entering sensitive information online, especially on a page you are not familiar with.

Best Practices for Using QueenWatcher

1. **Treat it as one signal among many** - Combine QueenWatcher's warnings with your own judgment, browser warnings, and other security tools.
2. **Pay attention to specific findings** - The detailed breakdown in the popup is more useful than the raw score. A single "Phishing Form" warning about password submission to an external domain is more actionable than a generic "High Risk" score.
3. **Context matters** - A news website with many external scripts may score higher than a simple blog, even though both are safe. Consider what kind of site you're visiting.
4. **Report issues** - If you consistently see false positives on legitimate sites, or if QueenWatcher misses something malicious, this feedback helps improve the tool.
5. **Don't disable other protections** - QueenWatcher complements, but does not replace, browser security features, antivirus software, or common sense.

Privacy

QueenWatcher operates entirely locally in your browser. It does not:

- Send your browsing history to any server
- Collect personal information
- Use external APIs or cloud services
- Track your online activity

All analysis is performed on your device, and all data (including scan history and settings) is stored locally in your browser.

Personal License

QueenWatcher is free for personal use.

Please contact Adsumsoft (via https://adsumsoft.nicepage.io) if you are planning to adopt it in a business setting.

Support and Feedback

QueenWatcher is a work in progress. Your feedback is essential for improving detection accuracy and reducing false positives. If you encounter issues or have suggestions, please report them through the extension's support channel or directly to Adsumsoft.