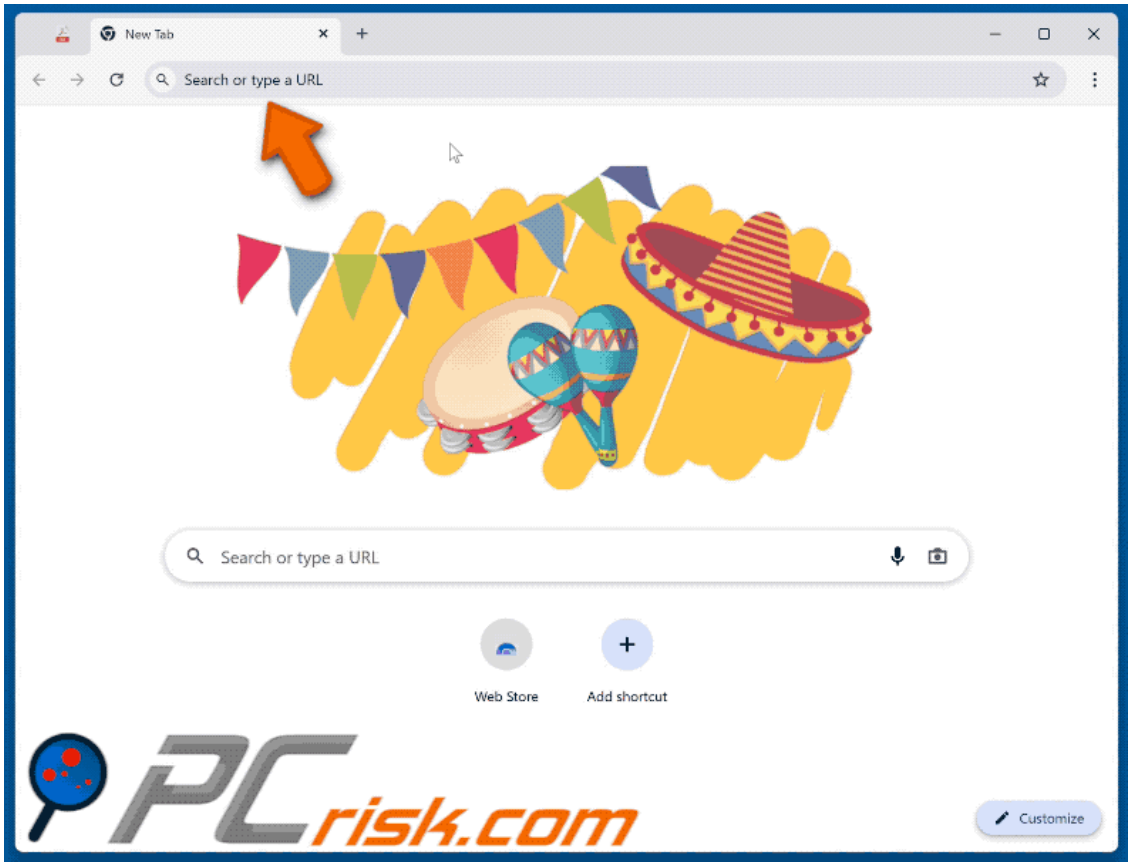
EpiBrowser: A Sophisticated PUP Masquerading as Chromium

EpiBrowser is a Potentially Unwanted Program (PUP) that can install on a victim's machine with or without their knowledge. To appear legitimate, it mimics Chromium-based browsers by using real Google Chrome components, most notably chrome_elf.dll, the library responsible for security initialization and system integration. It strengthens this deception with custom search engines (such as Yahoo!) and startup pages that mirror Chrome's look and feel, exploiting user trust in the familiar brand.



Here is a GIF preview of the EpiBrowser performing an unwanted search redirection to Yahoo! Search engine.
Courtesy of PCRisk.com

Todyl's EpiBrowser Findings

Observed Behaviors

- Creation and modification of COM-based scheduled tasks for automatic execution
- Registry autorun value manipulation to ensure boot-time activation
- File association changes to redirect user browsing activities
- Systematic reading of Internet Explorer security settings to map the browser environment
- Proxy server configuration analysis to understand network routing and potential bypass mechanisms
- Privacy and security setting modifications to reduce detection likelihood.

We also notice that it creates and subsequently terminates WerFault.exe (Windows Error Reporting service) during execution based on the samples' behavior, which is a technique commonly associated with process hollowing or injection attacks.

Certificate Abuse

The threat actor signed the software using certificates issued to 'Byte Media Sdn. Bhd.,' a Johor, Malaysia–based digital transformation consultancy that provides IT modernization, usability, and advisory services.

What is the present and future impact?

Users tricked into installing this browser become victims of data collection and search redirection. They may also risk potential exposure to additional malware through sketchy ads and search results.

The certificate abuse is particularly concerning because it's eroding one of our core trust mechanisms. If attackers can consistently obtain legitimate certificates from multiple CAs, the community may need to rethink our code signing verification approach entirely. With more malware families adopting these Chrome-mimicking techniques, EpiBrowser is a preview of what's coming, and we need to start preparing our defenses accordingly.

Guidance for MSPs

- Monitor for unexpected modifications to browser settings and autorun registry entries
- Exercise extreme caution when installing browser software from unfamiliar sources
- Regularly audit installed programs and browser extensions
- Monitor system startup programs for unexpected entries

Removal

Windows users can remove the browser from their system through the "Apps and Features" and "Programs and Features" options on Windows 11 and Windows 10, respectively.

Todyl Platform Capabilities

Todyl's security solution is designed to detect this specific type of cyber threat with precision. Backed by our expert MXDR team, we provide continuous monitoring of suspicious activity to quickly identify potential threats and safeguard your most sensitive assets. We also collaborate closely with your team to develop custom detection rules, ensuring full visibility, transparency, and a security approach tailored to your unique environment.

Indicators of Compromise

- The subject name of code signature is “Byte Media Sdn. Bhd."
- `(HKEY_CURRENT_USER\Software\EPISoftware\EpiBrowser*)`
  `(HKEY_CURRENT_USER\Software\EPISoftware\Update*)`
  `(HKEY_CURRENT_USER\SOFTWARE\Policies\EPISoftware\EpiBrowser)`
  - Description: Epibrowser registry persistence
- `C:\Users\<USER>\AppData\Local\Temp\epibrowser-bin\epibrowser.exe`
  `C:\Users\`
  `<USER>\AppData\Local\EPISoftware\EpiBrowser\Application\130.0.6723.147\notification_helpe`
  - Description: The file locations of the application.

References

1. https://www.malwarebytes.com/blog/detections/pup-optional-epibrowser
2. https://www.truesec.com/hub/blog/tamperedchef-the-bad-pdf-editor
3. https://www.wipersoft.com/remove-epistart-epibrowser-potentially-unwanted-program/

Hashes

1. `f52ca24fd5f99891e0385959bad2ddd9`
2. `14040c0474ba5e16c6d4d6fc20181d5e`
3. `184f49cade4b27dc435fe24f18d31f14`
4. `10a3f5c065831b6c889b289c5aacb02d`
5. `60b336093ae1c56e9bcd3b8322533101`
6. `ed5dc60c6dfda6b4ca321f147369de68`
7. `73c97542fe54228ea553be487a8d1665`
8. `97222a357a9f423ef3eee840154af91e`
9. `Dc03f86386c876231cef5e82c78ab75f`

About Ahsan

Ahsan Ayub is a Security Research Engineer at Todyl with over 8 years of combined industry and research experience in Software Development, Cybersecurity, and AI. He is passionate about applying AI to solve real-world cybersecurity challenges, investigating security concerns within AI systems, and developing expertise in both defensive and offensive security practices.

Ahsan earned his Ph.D. from Tennessee Tech University with a focus on Cybersecurity and AI. Prior to joining Todyl, he worked as a Security Engineer at Vanderbilt University Medical Center (VUMC). He has published more than 10 peer-reviewed scholarly articles covering topics including ransomware, malware, cryptography, adversarial machine learning, responsible AI, domain generation algorithms (DGA), and network covert communication.

Outside of work, Ahsan enjoys traveling, playing sports, and connecting with people.