This browser claims “perfect privacies protection,” but it acts like malware

The Universe Browser makes some big promises to its potential users. Its online advertisements claim it’s the “fastest browser,” that people using it will “avoid privacy leaks” and that the software will help “keep you away from danger.” However, everything likely isn’t as it seems.

The browser, which is linked to Chinese online gambling websites and is thought to have been downloaded millions of times, actually routes all Internet traffic through servers in China and “covertly installs several programs that run silently in the background,” according to new findings from network security company Infoblox. The researchers say the “hidden” elements include features similar to malware—including “key logging, surreptitious connections,” and changing a device’s network connections.

Perhaps most significantly, the Infoblox researchers who collaborated with the United Nations Office on Drugs and Crime (UNODC) on the work, found links between the browser’s operation and Southeast Asia’s sprawling, multibillion-dollar cybercrime ecosystem, which has connections to money-laundering, illegal online gambling, human trafficking, and scam operations that use forced labor. The browser itself, the researchers says, is directly linked to a network around major online gambling company BBIN, which the researchers have labeled a threat group they call Vault Viper.

The researchers say the discovery of the browser—plus its suspicious and risky behavior—indicates that criminals in the

region are becoming increasingly sophisticated. “These criminal groups, particularly Chinese organized crimes syndicates, are increasingly diversifying and evolving into cyber enabled fraud, pig butchering, impersonation, scams, that whole ecosystem,” says John Wojcik, a senior threat researcher at Infoblox, who also worked on the project when he was a staff member at the UNODC.

“They’re going to continue to double down, reinvest profits, develop new capabilities,” Wojcik says. “The threat is ultimately becoming more serious and concerning, and this is one example of where we see that.”

https://arstechnica.com/security/2025/10/this-browser-claims-perfect-privacies-protection-but-it-acts-like-malware/