**Annotated Bibliography**

Kerby Guillaume

# **“**[**Over 40 Malicious Firefox Extensions Target**](https://thehackernews.com/2025/07/over-40-malicious-firefox-extensions.html)

# [**Cryptocurrency Wallets, Stealing User Asset**](https://thehackernews.com/2025/07/over-40-malicious-firefox-extensions.html)**”**

Lakshmanan, R. (2025, July 3). *Over 40 Malicious Firefox Extensions Target Cryptocurrency Wallets, Stealing User Assets*. The Hacker News. <https://thehackernews.com/2025/07/over-40-malicious-firefox-extensions.html>

Ravi Lakshmanan’s article, recently published in July 2025, demonstrates a recent report where cybersecurity investigators uncovered a campaign involving more than 40 malicious Firefox extensions designed to steal users’ crypto wallet credentials. It was discovered that these extensions used false ratings to create trust, cloned branding, and code injection to extract sensitive crypto data. Lakshmanan provides detailed insight of potential risks targeted towards browser extensions in addition to corporate responses to these forms of cyber attacks.

# **“China-linked hackers spoof big-name brand websites to steal shoppers' payment info”**

Antoniuk, D. (2025, July 2). *China-linked hackers spoof big-name brand websites to steal shoppers’ payment info*. Therecord.media; The Record. <https://therecord.media/china-linked-hackers-website-phishing?&web_view=true>

Daryna Antoniuk’s article exposes a widespread phishing attack that targeted English consumers using Chinese code. Researchers from Silent Push identified thousands of fake retail websites impersonating major brands like Apple, PayPal, Nordstrom, Hermes, and Michael Kors; targeting consumers in order to obtain payment information. This article brings attention to the use of phishing across “trusted” brand sites in studying the methods hackers use to retrieve desired information.

# **“North Korean Hackers Use Fake Zoom Updates to Install macOS Malware”**

‌Ionut Arghire. (2025, July 3). *North Korean Hackers Use Fake Zoom Updates to Install macOS Malware*. SecurityWeek.

<https://www.securityweek.com/north-korean-hackers-use-fake-zoom-updates-to-install-macos-malware/>

Ionut Arghire’s article demonstrates another case of a phishing attack using different tactics to target its victims. In this case, attackers impersonate trusted contacts via Telegram and invite victims to fake Zoom meetings scheduled through Calendly. In order to join the meetings, the users were prompted to install a “Zoom SDK update” which was an AppleScript used to steal browser logs.

# **“Hawaiian Airlines Hit by Cyber Attack”**

Reuters. (2025). *Hawaiian Airlines Hit by Cyber Attack*. US News & World Report; U.S. News & World Report.

https://money.usnews.com/investing/news/articles/2025-06-26/hawaiian-airlines-hit-by-cyber-attack

‌The Reuters’ article, reported by David Shepardson, shows a report of an incident where hackers attacked the data systems of Hawaiian Airlines. Luckily, according to the Federal Aviation Administration (FAA), there were no safety impacts on the actual flight itself. This article includes statements from both the FAA and Hawaiian Airlines, highlighting the company’s engagement with cybersecurity experts and federal authorities. Reports such as Shepardson’s, demonstrates and brings understanding to the broad range of cyberattacks and specifically how aviation companies manage public communication during cybersecurity breaches.