WEEVILPROXY: An evasive and sophisticated malware campaign silently targeting crypto users across the globe

By Mohammad Kazem Hassan Nejad 27.06.2025 Mohammad: LinkedIn Share

Archived: 2026-04-05 13:21:28 UTC

WithSecure™ has uncovered a highly sophisticated and evasive malware campaign that has flown under the radar since March 2024.

The malware campaign targets cryptocurrency users, a user base estimated to be in the hundreds of millions which has emerged as a viable and effective lure to infect users and organizations across all sectors alike.

The campaign targets victims globally, with infections observed across each continent. Although the campaign targets cryptocurrency users, WithSecure has observed non-cryptocurrency-related organizations in Europe being infected by the malware due to cross-contamination introduced by personal browsing of victims on their corporate machines.

This is the latest campaign adopting the successful technique of propagating malware through large-scale pervasive ad campaigns displayed throughout the Internet in the form of images and videos using Google Display Network and social media platforms, such as Facebook and Twitter. These ads are estimated to have reached at least tens of thousands of users across the globe.

The initial stage of infection is primarily masked as popular cryptocurrency-related software and platforms, such as Binance, ByBit, TradingView, and more. However, business-oriented themes have also been deployed through Google ads.

Since its inception, the malware has been in constant and iterative development by the threat actor. Likely driven by its success so far, the threat actor has put in concerted effort to develop the malware’s breadth of capabilities, including novel techniques not observed in any prior malware campaigns - to our knowledge. These new TTPs include methods to modify Windows Setup and Windows Recovery to enable long-term persistence, as well as methods to patch browser extensions ‘on the fly’.

The extensive user tracking, the breadth of capabilities, the levels of obfuscation, and the sophistication of the campaign indicate a level of professionalism and innovation that’s often not observed in other equivalent malware campaigns, especially from a non-state actor. This is further emphasized by the usage of modern technologies, frameworks, and libraries by the threat actor throughout the campaign, including its usage of PostHog, Grafana, LevelDB, and tRPC, which are often observed in enterprise-level software and not leveraged by threat actors.

While the threat actor’s primary goal with the malware is to target cryptocurrency users, the malware’s extensive capabilities and threat actor’s skillset do not limit the threat actor to a specific goal for financial gain and pose a real threat to organizations and users across the globe alike. Furthermore, the lucrative nature of cryptocurrency

continues to drive advancements and innovation of ever more professional adversaries as noted by the set of novel features implemented in this campaign.

In this report, we provide a detailed breakdown of the delivery vector, the initial stage of the attack chain, and functionalities we have noted during our analysis of the main payload. MITRE ATT&CK TTP mapping and a full list of Indicators of Compromise (IOCs) can be found in the appendices.
