'Vortax' Meeting Software Builds Elaborate Branding, Spreads Infostealers

By Elizabeth Montalbano

Published: 2024-06-20 · Archived: 2026-04-05 16:19:37 UTC

Source: Klaus Ohlenschlaeger via Alamy Stock Photo

A widespread campaign aimed at stealing cryptocurrency is spreading a wave of infostealers through fake virtual meeting software for both macOS and Windows platforms, particularly targeting the former with the dangerous Atomic stealer.

Discovered by Recorded Future's Insikt Group, the campaign attributed to a threat actor dubbed "Markopolo" is responsible for an elaborate Web and social media presence for a fake app called Vortax, according to a report (PDF) published this week.

Vortax is purported to be virtual meeting software for various platforms but actually is a delivery mechanism for three infostealers: Rhadamanthys, Stealc, and Atomic, the researchers found. Attackers target cryptocurrency users in the campaign through social media and Telegram channels for the purpose of stealing credentials, so they can in turn steal crypto from them, according to Insikt.

The campaign is connected to a previously reported attack by Markopolo, identified then only as a Russian-speaking threat group, that previously targeted the Web3 gaming community. The group is known for using shared

hosting and command-and-control (C2) infrastructure in order to be able to pivot agilely to new scams when detected, according to Insikt.

"The campaign indicates a widespread credential-harvesting operation, potentially positioning Markopolo as an initial access broker or 'log vendor' on Dark Web shops like Russian Market or 2easy Shop," Insikt Group wrote in a blog post associated with the report.

The activity also demonstrates an uptick in infostealers that target macOS, which traditionally have been less prevalent than their Windows counterparts, Insikt Group noted in its report. Reports of Atomic stealer in particular have been on the rise based on recent research.

"The high volume of [Atomic] activity observed in this campaign builds on previous Insikt Group reporting, which found that mentions of macOS malware and exploit kits increased by 79% year-on-year from 2022 to 2023," according to the report. This "may indicate" a link between the overall number of references to macOS malware and the increased frequency of Atomic stealer campaigns observed in the wild, the researchers noted.

Vortax: Threats Hiding Behind a Convincing Brand

The foundation of the campaign is in Vortax, a fake "self-proclaimed" virtual meeting software marketed as cross-platform and AI-enhanced for which attackers built a convincing online brand. All major search engines index Vortax, which has a presence (@VortaxSpace) on social media platforms and even maintains a Medium blog using what are likely AI-generated articles.

The company behind the software claims to operate out of an address in Toronto that is actually an apartment building, and even boasts online about bogus awards from respected publications such as Forbes. However, closer inspection revealed that Vortax is a fraud, particularly shown by related website domains, vortax.io and vortax.space — the latter of which has since been suspended — that are rife with spelling and grammatical errors, according to Insikt.

Vortax advertises applications for Windows, Linux, macOS, iOS, and Android on its sites, though users cannot actually download the applications without a “Room ID," which functions as a meeting invitation.

Accounts associated with Vortax have four primary methods for sharing Room IDs — the most common of which are R12307012, R39264552, R87103129, and R71231209. These methods include: replies to the Vortax account on social media; direct messages on social media; posting in cryptocurrency-related Telegram channels; and posting in cryptocurrency-themed Discord channels.

These IDs ultimately lead to an installer for downloading Vortax, which as described just a front for delivering infostealing malware. On Windows platforms, the fake software delivers Rhadamanthys and Stealc, while it loads the Atomic stealer on macOS platforms.

To the user, it appears that Vortax is never actually installed, with the installation process "claiming that it encounters critical errors that impede it from running," while the software is actually "running many malicious processes" in the background, according to the report.

Mitigation Against Malware-Hiding Software

Insikt made a number of suggestions for mitigating the campaign, particularly across the macOS platform — which increasingly is being targeted and thus demands new vigilance and "robust defense strategies," according to the report.

Indeed, the distribution of Atomic stealer, previously distributed via fake software updates, demonstrates a pivot by by infostealing threat actors to macOS. One mitigation for the campaign, then, is to ensure that detection systems for Atomic infostealer are regularly updated to prevent infections, according to Insikt.

Organizations also should educate users on the risks of downloading unapproved software, especially from social media or search engines, and implement strict security controls to prevent employees from doing so. They also should encourage corporate network users to report suspicious activities encountered on social media and other platforms.

According to Insikt Group, using intelligence and monitoring platforms that scan for malicious domains and IP addresses associated with Atomic stealer and other macOS malware also can help prevent infection.

About the Author

Contributing Writer

Elizabeth Montalbano is a freelance writer, journalist, and therapeutic writing mentor with more than 25 years of professional experience. Her areas of expertise include technology, business, and culture. Elizabeth previously lived and worked as a full-time journalist in Phoenix, San Francisco, and New York City; she currently resides in a village on the southwest coast of Portugal. In her free time, she enjoys surfing, hiking with her dogs, traveling, playing music, yoga, and cooking.

Source: https://www.darkreading.com/remote-workforce/vortax-meeting-software-branding-spreads-infostealers