

The Travels of “markopolo”: Self-Proclaimed Meeting Software Vortex Spreads Infostealers, Unveils Expansive Network of Malicious macOS Applications

recordedfuture.com/the-travels-of-markopolo-self-proclaimed-meeting-software-vortex-spreads-infostealers

Research (Insikt)

Posted: 17th June 2024

By: Insikt Group®



Recorded Future's Insikt Group identified that Vortex, a purported virtual meeting software, spreads three infostealers—Rhadamanthys, Stealc, and Atomic macOS Stealer (AMOS). This extensive campaign targets cryptocurrency users, exploiting macOS vulnerabilities. Operated by the threat actor “markopolo,” this campaign has significant implications for macOS security, indicating a potential increase in AMOS attacks.

The Travels of “markopolo”: Self-Proclaimed Meeting Software Vortex Spreads Infostealers, Unveils Expansive Network of Malicious macOS Applications

While monitoring data in Recorded Future Malware Intelligence, Recorded Future's Insikt Group has identified a widespread cyberattack campaign involving Vortex, a supposed virtual meeting software. Once downloaded and installed, Vortex delivers three potent information stealers—Rhadamanthys,

Stealc, and Atomic macOS Stealer (AMOS). This campaign, primarily targeting cryptocurrency users, marks a significant rise in macOS security threats and reveals an expansive network of malicious applications.

Key Findings

- Vortex and its associated applications have been used in extensive campaigns aimed at cryptocurrency theft, significantly impacting macOS users. The campaign connects to a previously reported campaign targeting Web3 gaming, suggesting the same threat actor ("markopolo") is behind both.
- markopolo uses shared hosting and C2 infrastructure for agility, quickly pivoting to new scams when detected.
- 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.

Mitigations

- Ensure that detection systems for AMOS are regularly updated to prevent infections.
- Educate users on the risks of downloading unapproved software, especially from social media or search engines.
- Implement strict security controls to prevent the download of unlicensed software.
- Encourage users to report suspicious activities encountered on social media and other platforms.
- Recorded Future clients can use Recorded Future Malware Intelligence to identify and mitigate threats from malicious macOS applications, analyzing connections to AMOS C2 infrastructure. Combined with Recorded Future Network Intelligence, it helps identify malicious domains and IP addresses associated with AMOS builds.
- Monitoring technology stacks through custom watch lists in Recorded Future Intelligence Cloud, Threat Map, Vulnerability Intelligence, and Attack Surface Intelligence enhances visibility into infostealer threats.
- Additionally, Recorded Future Identity Intelligence and Brand Intelligence provide insights into compromised credentials from AMOS infostealer logs, database breaches, and combo lists.

This campaign demonstrates the adaptability and scalability of modern cyber threats. As demand for macOS malware increases, organizations must shift their perception of macOS security and adopt robust defense strategies.

Monitoring and mitigating such threats will be crucial in maintaining a secure digital environment.

To read the entire analysis, [click here](#) to download the report as a PDF.

Related