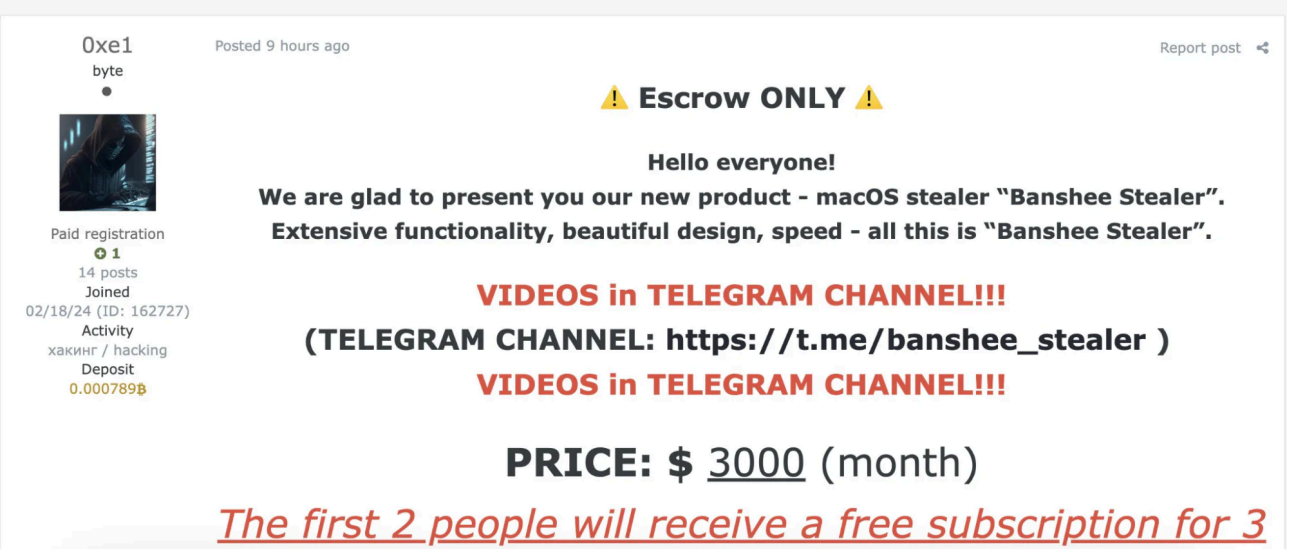
The source code of Banshee Stealer leaked online

By Pierluigi Paganini

Published: 2024-11-26 · Archived: 2026-04-06 00:42:06 UTC

Pierluigi Paganini November 26, 2024



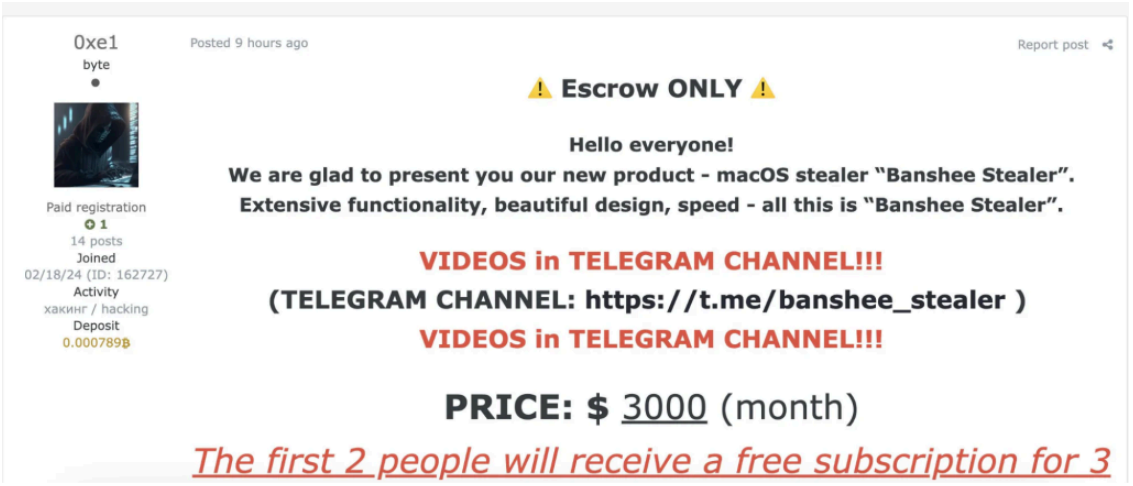
Banshee Stealer, a MacOS Malware-as-a-Service, shut down after its source code leaked online. The code is now available on GitHub.

In August 2024, Russian hackers **promoted** BANSHEE Stealer, a macOS malware targeting x86_64 and ARM64, capable of stealing browser data, crypto wallets, and more.

BANSHEE Stealer supports basic evasion techniques, relies on the sysctl API to detect debugging and checks for virtualization by running a command to see if "Virtual" appears in the hardware model identifier.

The malware avoids targeting Russian systems by checking the user's language settings via the CFLocaleCopyPreferredLanguages API, though this can be bypassed.

The discovery of the malware highlights the growing focus on macOS-specific malware as the platform becomes a more frequent target for cybercriminals.



Researchers at Elastic Security Labs analyzed the malware and confirmed it can steal keychain passwords and data from multiple browsers.

Banshee Stealer can target data from nine different browsers, Chrome, Firefox, Brave, Edge, Vivaldi, Yandex, Opera, OperaGX, and Safari. The malware can collect cookies, logins and browsing history, but from Safari only cookies can be collected. Elastic researchers noticed that regarding Safari, only the cookies are collected by the AppleScript script for the current version.

*"Additionally, data from approximately 100 browser plugins are collected from the machine. A list of these extension IDs is provided at the end of the blog post." reads the **report** published by Elastic Security Labs. "The collected files are saved under <temporary_path>/Browsers."*

Banshee Stealer can also steal cryptocurrency from different wallets, including Exodus, Electrum, Coinomi, Guarda, Wasabi Wallet, Atomic and Ledger.

After collecting data, the malware compresses the temporary folder containing them into a ZIP file using the ditto command. The ZIP file is then XOR encrypted, base64 encoded, and sent via a POST request to a specified URL using the built-in cURL command.

"BANSHEE Stealer is macOS-based malware that can collect extensive data from the system, browsers, cryptocurrency wallets, and numerous browser extensions." concludes the report. "Despite its potentially dangerous capabilities, the malware's lack of sophisticated obfuscation and the presence of debug information make it easier for analysts to dissect and understand. While BANSHEE Stealer is not overly complex in its design, its focus on macOS systems and the breadth of data it collects make it a significant threat that demands attention from the cybersecurity community."

This week, the source of the Banshee Stealer, the MacOS-based Malware-as-a-Service (MaaS) infostealer, has been leaked online, researchers at VXunderground reported.

The operators behind the MaaS have shut down their operations after the data leak.

VXunderground archived the leak and published it on GitHub.

“Yesterday Banshee Stealer, the MacOS-based Malware-as-a-Service infostealer, had their source code leaked online. As a result of the leak they’ve shut down their operations. We’ve archived the leak and made it available for download on GitHub.”

Follow me on Twitter: **@securityaffairs** and **Facebook** and Mastodon

Pierluigi Paganini

(SecurityAffairs – hacking, BANSHEE Stealer)
