AL2025_11 PirateFi Malware Attack on Steam: Vidar Infostealer Compromises Users (18th February 2025)

Description

PirateFi, a free-to-play survival game on Steam, was found to contain the Vidar infostealing malware, putting up to 1,500 users at risk. The game was available for download between February 6 and February 12, 2025, before being removed by Steam. PirateFi was marketed as a low-poly survival game featuring base-building, weapon crafting, and food gathering. However, it was discovered that the developer, Seaworth Interactive, had uploaded game builds laced with malware. As a result, Steam has advised affected users to take urgent security measures, including reinstalling their operating system.

Attack Details

The malicious game was hosted on Steam and initially received positive reviews. Steam identified the presence of malware in the game files but did not specify the type. Security researchers later confirmed that PirateFi was distributing the Vidar infostealer, a malware variant designed to steal sensitive user data, including credentials, session cookies, and cryptocurrency wallet information.

The malware was embedded within the game's executable file, Pirate.exe, where it deployed a payload (Howard.exe) using an InnoSetup installer. The attackers frequently modified the game files and changed their command-and-control (C2) servers to evade detection. The name "PirateFi" appears to have been deliberately chosen to attract cryptocurrency enthusiasts due to its association with Web3 and blockchain.

Remediation

Users who downloaded and played PirateFi should take immediate action to secure their systems and accounts:

- Run a Full System Scan – Use an up-to-date antivirus or anti-malware software to detect and remove any malicious files.
- Format and Reinstall Windows – To ensure complete removal of any residual malware, reinstalling the OS is strongly recommended.
- Change All Compromised Passwords – Update credentials for email, banking, gaming, and cryptocurrency accounts. Use a password manager for secure storage.
- Enable Multi-Factor Authentication (MFA) – Strengthen account security by enabling MFA wherever possible.
- Monitor for Unusual Activity – Keep an eye on financial and personal accounts for any unauthorized transactions or access attempts.
- Check for New Software Installations – Review installed applications and remove any unknown or suspicious programs.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Kan, M. (2025, February 12). Did you download this Steam game? Sorry, it's Windows malware. Retrieved from PCMAG. https://www.pcmag.com/news/did-you-download-this-steam-game-sorry-its-windows-malware
- Toulas, B. (2025, February 15). PirateFi game on Steam caught installing password-stealing malware. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/piratefi-game-on-steam-caught-installing-password-stealing-malware/