



Fullerton College

Emerging Technology Lab: Briefing on PirateFi

Executive Summary

This briefing examines the 2025 malware incident known as “PirateFi”, which was discovered through the Steam gaming platform. The malware caused widespread issues, including data theft, unauthorized access to digital wallets, and compromised user credentials. The attack impacted thousands of users and exposed weaknesses in Steam’s content moderation and malware detection systems. The briefing covers the origins and impact of PirateFi, the specific systems affected, the issues victims faced, reveals the extension of social engineering, and highlights the growing risks within the gaming industry due to vetting processes and malware distribution. It mentions how incidents like this are preventable and concludes with best security practices for both individuals and organizations. The methods organizations use to share data and their impact is evaluated. The briefing recommends users to use antivirus tools, cautious internet use, and security layers like multi-factor authentication. PirateFi serves as a critical case study in the importance of cybersecurity preparedness and is a reminder that dangerous malware can bypass systems if not secured efficiently.

PirateFi

A malware infested game titled *PirateFi* was published on Steam, a popular game distribution platform owned by Valve. *PirateFi* was available for free and up for 6 days until it was removed on February 12, 2025; after discovering it contained an information stealer named *Vidar*. Although, the game had already been downloaded by an estimated 800 – 1,500 users. The game was listed by developer, SeaWorth Interactive who had little to no online presence. The developer did not have any other published games and the game’s Steam page had been created just 18 days (about 2 and a half weeks) before its release. *PirateFi* was announced just weeks before its launch and only by Steam. Solo/independent games are usually announced months before and major game titles, years in advanced.

The short timeline was concerning but the game initially warded off suspicions with positive reviews and a high rating of 9/10. Reviewers praised the game for being engaging, even encouraging the use of the multiplayer feature, likely to increase downloads. Their false legitimacy was based on deception, all tactics to make users overlook the red flags. Seaworth Interactive took advantage of the trusted platform and loyal users. Steam has strong credibility with an estimated 69 million daily users and an average of 28 games released to the platform per day, making it easy for victims to download without hesitation.

Popularity is not what should establish your trust between a company, publishing on Steam is easier than some may think. Developers do not have to be established. Anybody can publish a game on Steam for a fee of \$100 USD per game and basic documentation. A functioning build of the game, store assets (trailer, screenshots, description) and a valid bank account for payout must be provided. Valve also does a brief review for technical issues, legal concerns, and malicious behavior like previous offensives but not for game quality. The process only takes a few days which explains why *PirateFi* did not have a prior online presence, it was unnecessary.

PirateFi was advertised as a survival game where players could take on the role of a pirate in single and multiplayer modes. Their steam profile included in-game screenshots and a trailer, but it was not *PirateFi*'s original content. It deceived the public by modifying an already existing video game to become *PirateFi*. An existing template of a game titled *Easy Survival RPG* was used, described as "game-making app that gives you everything you need to develop your own singleplayer or multiplayer game." This is known as "asset flipping," where developers use pre-made assets to quickly create and publish games. The game maker costs between \$399 and \$1,099 to license. A small price to pay in return for stolen data from every device that downloaded the game.

PirateFi Problems

The malware it was infested with, Vidar, is an information stealer designed to steal information from a person's computer or device. When included in pirated software, Vidar infiltrates systems upon installation and collects sensitive data like passwords and other credentials stored in browsers or password managers. This stolen information is then uploaded to the attackers' servers. Vidar is capable of stealing session tokens from the users' browser, enabling attackers to gain access without needing their password or multifactor authentication code. It can also steal cryptocurrency wallet details, data from web browser autofill features, screenshots, and other files.

Regarding *PirateFi*, Marcus Genheimer, a researcher from SECUINFRA Falcon Team stated, "We suspect that *PirateFi* was just one of multiple tactics used to distribute Vidar payloads en masse," He added that it was "highly unlikely" *PirateFi* was ever a legitimate, running game before it was altered.

PirateFi was not the first Vidar incident, Vidar was discovered in 2018 and “grown to be one of the most successful infostealers.” The malware has been used in several company hackings; there was an attempt to steal Booking.com’s hotel credentials and others with the goal of deploying ransomware and malicious advertisements on Google search results.

Infostealers like Vidar are usually sold as in the malware-as-a-service model, it can be purchased and utilized by low-skilled hackers or armatures. The widespread adoption of infostealers makes it exceedingly difficult to trace whoever was behind *PirateFi*, as it has been embraced by numerous cybercriminals. Another method *PirateFi* used to lure victims was through Telegram, falsely advertising a \$17-an-hour pay rate for users to play the game.

Telegram is a cloud-based messaging platform that offers end-to-end encrypted chats, file sharing, and group messaging. It is known for privacy and security, explaining their more than 700 million active users. While it is often used for casual conversations, it has become a popular platform for spaces where anonymity is valued. This includes community engagement, business discussions, and content related to politics, activism, entertainment, and technology. Similar to platforms like Steam, Telegram is highly trusted but lacks strict content moderation despite being promoted as a secure option. Oversight has turned Telegram into a playground for cybercriminals, where malicious links, software and services are distributed to promote malware such as Vidar. In *PirateFi*’s case, the attackers exploited Telegram’s wide reach to recruit more victims into downloading Vidar by playing the game.

Systems Affected

A user reported that their antivirus flagged the download as 'Trojan:Win32.Lazzy.gen.' The malware was also noted to unpack into /AppData/Temp/****/ and appeared as 'Howard.exe.' The malware allowed the hacker to hijack access of accounts when successful. Gamers discovered their accounts had been hacked; passwords changed, and accounts accessed through stolen browser cookies. When browser cookies are stolen attackers can hijack active login sessions, allowing them to access accounts without needing passwords or two-factor authentication. For example, if Google Chrome or Microsoft Edge is your default browser, you might already be logged into your Google or Microsoft account. This means attackers can gain access to your email, social media, or gaming platforms. In many cases, stolen cookies are bundled with other data and sold on dark web marketplaces for use in fraud, identity theft, or further attacks.

The malicious activity did not end with the initial breach. Once access was gained, the attacker exploited the compromised account’s friends list to spread malware further. Phishing links were sent to contacts on the victim's friends list through Steam, Discord, Microsoft, or email. These messages would appear to come from a trusted friend increasing the chances of others clicking and falling victim to Vidar. In some cases, hacked Microsoft accounts were drained of stored funds or subscriptions, and victims were even locked out entirely. Attackers would disable

recovery options or block access to Microsoft support channels, making account recovery difficult or impossible. This cascade effect turned a single infection into a broader social engineering campaign, amplifying the malware's impact.

The trojan was executed almost too easily. Considering hackers with limited technical skill can purchase and deploy the infostealers sold in the malware-as-a-service model, it is no surprise. According to user reports, Kaspersky Premium is the antivirus that identified the malware. When launching a game, Kaspersky automatically enters the “Game Mode” feature and disables any pop-ups, notifications, or suspicious activity. If the game does not behave normally, such as attempting to access critical system files or acting like malware, Kaspersky may block the game from launching or alert you to the potential threat.

Industry Implications

A highly reputable source with an absurd amount of network traffic remained unaware of the malware *PirateFi* was infected with until it was flagged by a user report. It made sense for hackers to target the steam platform because of their high user count but it is a lesson to always do your own due diligence. This is not just the responsibility of users. A growing distrust between users and gaming platforms has emerged which is an issue that affects not only the players but also the developers who rely on platforms like Steam to release their games.

Steam and by extension, Valve was unable to detect the malware at the time of *PirateFi's* release due to the way the platform handles game submissions. The malicious software was packaged using a legitimate installer tool, allowing it to slip past Steam’s automated validation systems. The lack of deep file scanning and the developer having no prior offenses, made the malware infected game remain unflagged. Steam’s heavy reliance on user reports further delayed detection. This incident exposed critical flaws in the platform’s security approach and served as a reminder that while automation streamlines processes, incorporating manual oversight from cybersecurity professionals remains essential.

Despite the breach caused by *PirateFi*, Steam's market dominance remains unchallenged. The platform continues to boast over 132 million monthly active users and 69 million daily active users as of 2025, with record-breaking concurrent user peaks exceeding 39 million in December 2024. Additionally, Steam's revenue reached an all-time high of \$10.8 billion in 2024, marking a 24% increase from the previous year.

There has been no direct accountability placed on Steam or its parent company, Valve, following the *PirateFi* incident. Public scrutiny has primarily focused on Vidar itself and the cybercriminals behind the distribution. It is appropriate to direct concern toward the incident from that perspective, but it should not divert attention from the role distribution game platforms play in enabling cyber threats. Valve has not faced measurable losses in profit or user engagement and there is a deeper industry problem: even when breaches occur, dominant

platforms rarely suffer meaningful consequences. There is little real competition in the PC gaming space and Steam is not financially pressured to improve oversight. Yet, the responsibility to protect loyal users remains and cybersecurity is an obligation that does not only risk long-term erosion of trust but contributes to availability of cybercrime.

Preventing PirateFi

Prevention is the foundation of cybersecurity, and it must be the guiding principle as Valve moves forward from this incident. To prevent similar breaches, Valve should implement stricter vetting processes for games before they are released. This could include comprehensive static and dynamic malware scans to detect hidden threats. However, not everything is captured in those scans, so continuous monitoring of live games is essential to flag suspicious activity and identify abnormal behaviors.

User reporting has proven to be a critical line of defense, so prioritizing a faster, more efficient response system is crucial. The quick identification of *PirateFi* was made possible through user vigilance, underscoring the need for streamlined reporting channels and swift action from platform support. Compromised users should be able to access immediate account support, and an automated system should be in place to revoke session tokens or invalidate account access when malicious activity is detected.

The malware attack experienced by Steam should push them in the direction of collaboration. Threat intelligence firms thrive on collaboration to share real-time threat data so systems can be stronger. Threat intelligence can integrate cybersecurity frameworks like MITRE ATT&CK, CVE, NIST cybersecurity Framework, CTI, and more. They will be able to stay ahead of evolving threats, block known malware strains, and prevent new variants from slipping through any flawed systems.

Best Security Practices

PirateFi was particularly deceptive because it understood before launching that users rely on reviews, ratings, and the publisher to establish trust before downloading a game. The creators ensured that these 3 indicators appeared normal at first glance. However, game reviews can be analyzed the same as phishing emails. Ask yourself:

- Are there any typos or awkward phrasing in the review?
- Does the reviewer have a history of posting other comments?
- Is the reviewer's account new or suspiciously lacking other activity?
- What is the timestamp of the post? Does it seem natural in relation to the game release?

The same logic should be applied to ratings. Opinions vary so it is unusual if a game does not have any negative feedback (bad review or rating). Make note of the total number of ratings-is it realistic? Do the reviews align with the overall rating, or are they one-word endorsements with perfect scores? These are anomalies that should raise suspicion.

When evaluating the publisher, question their familiarity and/or reputation. Do they have other known published games or is this their first? If they are not an established publisher, it can reveal that it might be a front for malware distribution as seen in the case of *PirateFi*.

Due diligence is a practice of prevention and can protect you from downloading malware. Hackers often think like a typical user and try their best to hide any red flags. This mindset is not reserved for downloading malware and should be applied for everyday security. It is important to be cautious while online as cyberattacks emerge as time passes. Hackers get more and more creative daily, do not be naïve and lookout for text messages, emails, clickable content, and social media scams. Be mindful of the outlined patterns to spot potential threats. Make a habit of updating your systems regularly, research what you do not know and follow cybersecurity awareness tips. Never forget to always use an antivirus to scan for malware or suspicious activity, as malware does not always execute immediately.

About Emerging Technology Lab

The Emerging Technology Lab offers hands-on, experiential learning opportunities designed to prepare students for real-world challenges in cybersecurity and information systems. The lab acts as a space for emerging technology and cybersecurity topics, presented through class courses, workshops and technical briefings. The Advanced Computer Topics course is a lab environment class taught by Professor Brian Roach, where students gain exposure to various functions of cybersecurity tools and computer systems. Since technology is ever evolving the labs taught in the course are not fixed and subject to change with relevance.

The hosted workshops are open throughout the year and are available to all interested students! Workshop sessions cover a wide range of topics, including password cracking, phishing awareness, patch management, Azure security, Windows Server installation, malware analysis, phishing, intrusion detection systems, OSINT, etc. Students gain direct experience with powerful tools and platforms like Kali Linux, Security Onion, Metasploit, and various Hak5 devices.

Technical briefings written and provided by the Emerging Technology Lab enable a community for everyone to be involved in cybersecurity news and practices. They analyze different cybersecurity breaches or incidents to educate on their causes and solutions. The briefings not only act as educational but also peak interest. Their purpose is to spread awareness so that nobody falls victim to these types of cybercrimes.