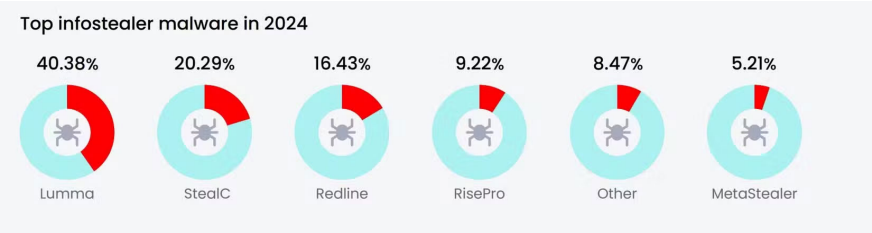
Why is Infostealer malware the biggest new malware concern?

Often distributed in a malware-as-a-service model, infostealer malware is often used to steal data, remaining hidden for as long as possible.

In recent years, people have been particularly wary of one type of malware: Infostealer. Often distributed as a malware-as-a-service, infostealer malware is often used to steal data, remaining hidden for as long as possible — and that's just one of the problems it can cause.

5. Infostealer malware targets private data

The first reason people are worried about infostealer malware is that in 2024, it caused a leak of 3.9 billion passwords in just one year! Security research firm KELA revealed the staggering figure in its State of Cybercrime 2024 report, along with the information that over 4.3 million devices were infected with infostealer malware.



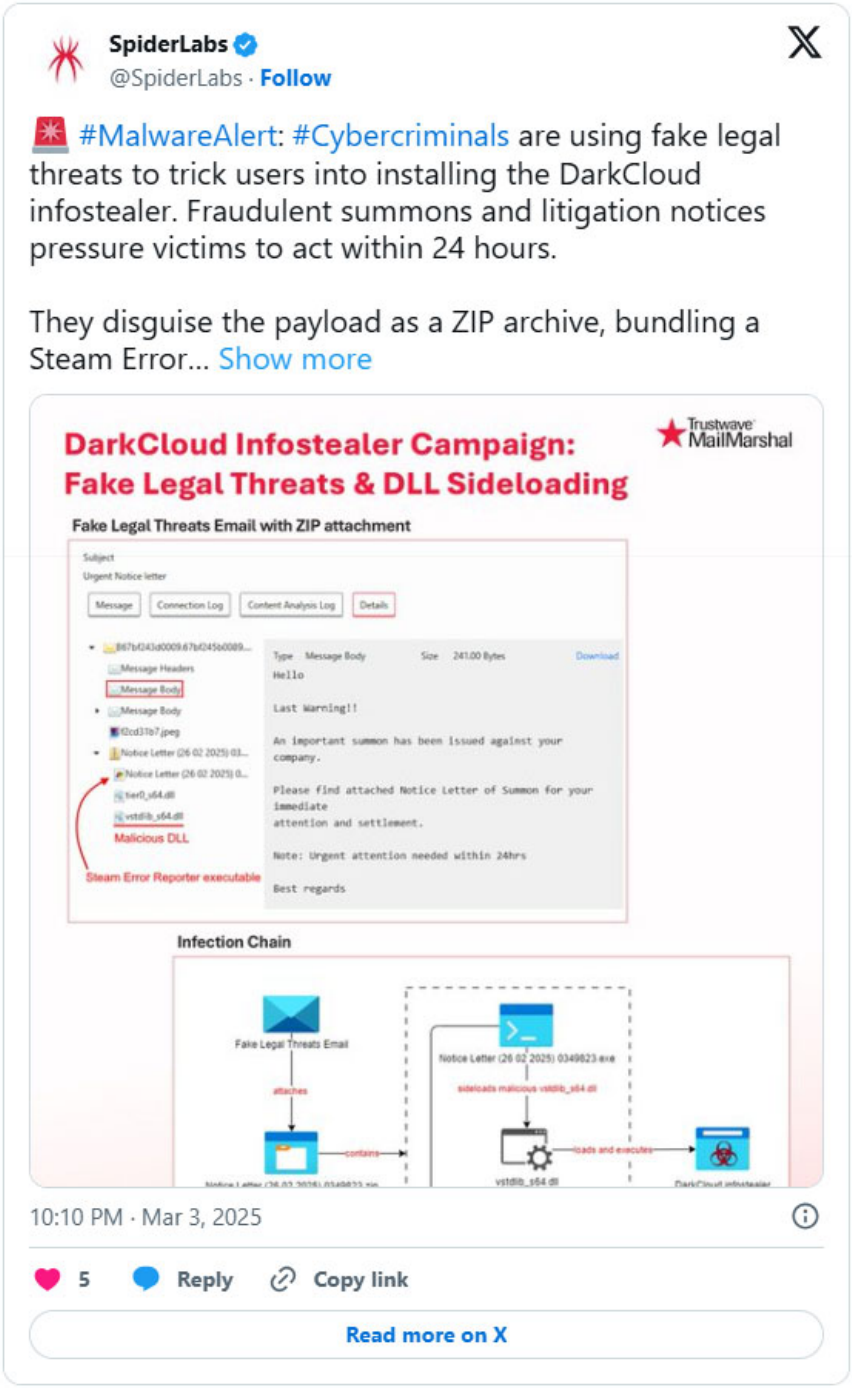
Then another security research firm, Huntress, released its 2025 Cyber ??Threat Report — and revealed that by 2024, ransomware will account for a staggering 25% of cyber attacks.

So while attackers have been using infostealer malware for a long time, it's only in the last few years that it's really ramped up.

4. Infostealer can silently steal a wide variety of sensitive data in large quantities

Another concern is that infostealers steal data extracted from multiple accounts of a single person. They can steal a lot of your sensitive data, including:

1. Personal data (address, phone number, social security number)
2. Email and chat logs
3. Browser data (history, cookies, bookmarks)
4. Financial information (bank details, credit card numbers)
5. Login information (username and password)
6. Cryptocurrency Account



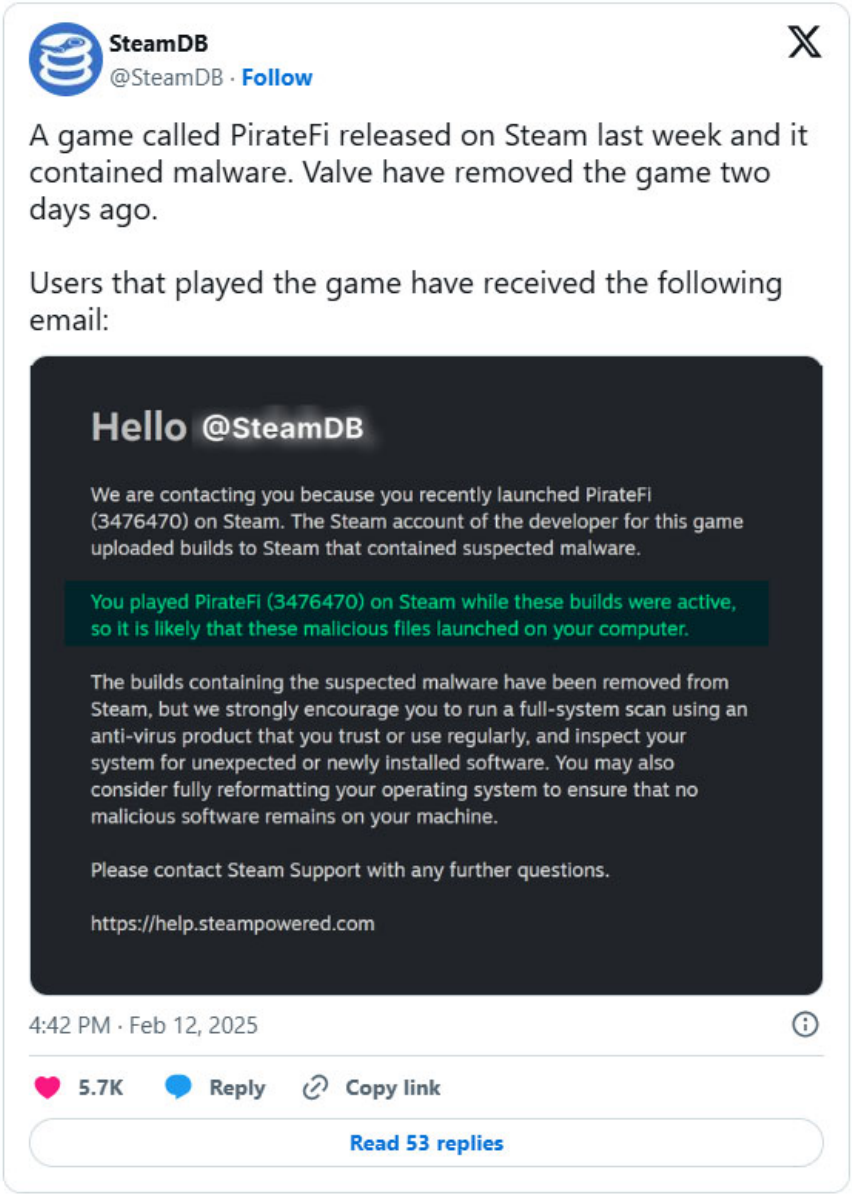
Some infostealer malware logs your keystrokes, like a snake keylogger, while others have clipboard hijacking capabilities to steal information you copy to your device's clipboard. Others have file harvesting components that go through your files and emails, and most have a screen capture feature that takes screenshots of you entering login credentials or having sensitive personal information on screen.

What's worse is that this infostealer can silently infect your system and do all this secretly without you even realizing anything suspicious is going on. Attackers also use advanced obfuscation techniques to avoid detection.

3. The threat of information theft is everywhere

Infostealer is distributed using both phishing and non-phishing methods, and is carried out on almost every popular platform. You'll see hackers trying to lure you into downloading infostealer malware on video-sharing sites like YouTube , social media apps like Facebook and LinkedIn , as well as fake email attachments or human-like verification pages.

Pirated software is the primary source of infostealer malware, as you might expect. However, there have also been examples of infostealer malware embedded in stolen software uploaded to legitimate websites. In February 2025, a game uploaded to Steam, PirateFi, was found to contain infostealer malware. Although Valve, the owner of Steam, quickly removed the free game from its platform, it had already infected hundreds of computers.



2. Malware infostealer is often used as a gateway for larger attacks

This is something to be really concerned about. Many sinister cybercrime attacks can be traced back to an initial infostealer infection. The malware acts as a reconnaissance tool for hackers to launch larger attacks, using the data gathered and initial access gained by infostealer.

For example, once hackers infect your work device with infostealer, they can steal your company credentials and gain access to your organization's network. They can then scan your system for other valuable data or install backdoors and remote access tools. Finally, they can steal a bunch of your company's data or encrypt it to cripple your operations and demand a ransom.

1. The threat of information theft is expected to increase

Widespread Infostealer infections are creating a global malware epidemic. According to Check Point's 2025 Cybersecurity Report, Infostealer malware has increased by 58%, with organizations in Europe, the Middle East, and Africa seeing a huge increase in attacks. Other continents are also facing the problem of information theft. For example, a campaign distributing InfoStealer SYS01 malware impacted millions of people globally, spanning regions including Australia, Asia, North America, and Europe.

With advanced obfuscation techniques and the use of AI to enhance phishing campaigns, the threat of information theft is expected to continue to grow in scale and sophistication. Infostealers like the infamous Lumma strain are expected to continue to plague individuals and businesses, so it is important to remain vigilant.

Malware infostealer isn't the only threat we face online. But it's certainly the one we should be most worried about right now!