Why is macOS becoming an increasingly attractive target for cybercriminals?

Reports indicate that malware targeting macOS is rapidly increasing, while Apple is cutting bug bounties for security vulnerabilities. Why is this trend dangerous, and what can Mac users do to protect themselves?

For years, Mac users held a tacit confidence that most malware wouldn't target them. This was true, but it's changing. Many cybersecurity companies report a significant increase in threats directly targeting macOS. Jamf notes that data-stealing malware is appearing more frequently on Macs. SentinelOne tracks a significantly higher number of new macOS malware variants than before. These are all companies that provide real data to corporate clients, not just hearsay.

The main reason lies in the number of users. The more popular Macs become, the more reason hackers have to invest in writing malware specifically for macOS. Info *-stealers* are particularly prevalent because they target exactly what cybercriminals can profit from most: saved browser passwords, login cookies, digital wallets, and account tokens. Previously, hackers mainly relied on adware or hijackers to make money from Macs. Now they see macOS like Windows: a platform large enough to warrant serious investment.

What should Mac users do when the threat escalates?

The good news is that most Mac users don't need to change their entire usage routine. Just start with the most important steps: always keep macOS and applications updated to the latest version, and enable automatic

updates. Apple's built-in protection system works best when always updated, but missing patches significantly weakens this protection.

Gatekeeper should be set to 'App Store and Developer Verified'. Regularly bypassing this warning just to install software from unknown sources is a habit that puts you at the greatest risk.

When downloading apps, maintain the same caution as on Windows: avoid cracked apps, fake installers, or tools that claim to be 'speed boosters' or 'magical junk cleaners'. Only download from reputable sources, and trust warnings from macOS or your browser.

Finally, stay realistic. There's no need to panic or install five layers of security, but acknowledge that macOS is indeed vulnerable to attacks. Maintaining a few healthy habits is enough to keep you safe from most threats.

Macs may still be safer than the average Windows machine, but the situation is changing rapidly. As attackers increasingly focus on macOS and Apple reduces incentives for security researchers, user initiative becomes more important than ever. There's no need to treat your Mac like a ticking time bomb; just keep it fully updated, install applications selectively, and listen to system alerts. A few good habits remain the most effective defense while the ecosystem continues to adapt.