**A password-cracking company claims to be able to crack passwords on Macs with the T2 security chip.**



In a nutshell, a password recovery company uncovered a weakness in Apple's T2 chip that allows it to conduct a brute-force attack to crack a Mac user's credentials. The process can still take a long time, but the company's software can unlock a Mac in as little as 10 hours if the password is weak.

Passware has been selling software-based hacking solutions for nearly two decades. Its tools are mostly utilised for legal purposes like forensics and data recovery. However, when Apple released their T2 security chip in 2018, Passware's solutions for macOS had a problem.

The T2 is a hardware-based gatekeeper that accepts only a limited number of password attempts before locking the system down. So the only way in is to crack the file system's decryption key, which even with GPU acceleration would take millions of years to brute-force.

A new module in Passware allows you to bypass the password attempt limiter. However, 9to5Mac points out that it's a bit slow. On previous Macs, the programme can process tens of thousands of guesses each second, while the new bypass module can only handle roughly 15 attempts per second. Despite this, the software can crack a relatively weak six-character password in around 10 hours using a 500,000-word dictionary assault.

Because physical access to the computer is necessary, the average user is only at risk from this T2 vulnerability. It also only works on Intel Macs with the T2 processor. The hack does not affect the newer M1 Macs, but earlier devices lacking the T2 are still vulnerable to previous versions of the tools.

Passware claims that it only offers its software to government agencies or private enterprises who can demonstrate that they have a legitimate need for it. It's also not letting the public know about the vulnerability.

However, now that the security flaw has been discovered, you can bet that hackers will rush to exploit it before Apple can close it down.